THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

A review of Costas arrays

Citation for published version:
Drakakis, K 2006, 'A review of Costas arrays', *Journal of Applied Mathematics*, vol. 2006, 26385, pp. 1-32. https://doi.org/10.1155/JAM/2006/26385

Digital Object Identifier (DOI):
10.1155/JAM/2006/26385

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Journal of Applied Mathematics

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

OPEN ACCESS

Download date: 07. May. 2023

A REVIEW OF COSTAS ARRAYS

KONSTANTINOS DRAKAKIS

Received 15 March 2005; Revised 13 January 2006; Accepted 5 March 2006

Costas arrays are not only useful in radar engineering, but they also present many interesting, and still open, mathematical problems. This work collects in it all important knowledge about them available today: some history of the subjects, density results, construction methods, construction algorithms with full proofs, and open questions. At the same time all the necessary mathematical background is offered in the simplest possible format and terms, so that this work can play the role of a reference for mathematicians and mathematically inclined engineers interested in the field.

Copyright © 2006 Konstantinos Drakakis . This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Costas arrays are a topic unique from some aspects: they are useful to engineers and fascinating to mathematicians interested in discrete mathematics, because of the many still open problems they present; furthermore, the effort devoted in their study resulted in new contributions in algebra, in the theory of finite fields [8, 14, 15, 22, 24]. But the researcher who would like to undertake research in the field will have first of all to overcome the hurdles posed by the fact that the literature on the topic spans two very broad fields (engineering and mathematics) and four decades, with all the consequences this may have. For example, some of the papers seem too practical for mathematicians, some too mathematical for engineers, while some, too old to make it to the era of electronic journals, are simply too hard to find.

The purpose of this review is to collect all main mathematical facts about Costas arrays, and to provide the background needed, in the simplest possible terms, to understand and prove them. In particular, this review will provide:

(1) a survey of our knowledge on Costas arrays today,
(2) an account of the different methods available today for their construction,
(3) proofs for the construction algorithms and the density results available today.

Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2006, Article ID 26385, Pages 1–32
DOI 10.1155/JAM/2006/26385

This review, on the contrary, will not mention results or provide proofs of results that require mathematical tools that are too advanced or are too complicated compared to the results' usefulness.

To sum up, this review is addressed to mathematically inclined engineers and mathematicians who would like to know (almost) all about Costas arrays; it is the result of the notes kept by an applied mathematician who wanted to know and understand (almost) all about Costas arrays.

2. Definition of Costas arrays and notation

In this paper the following notation will be used.

(i) $\{0,1\}^{n\times n}$, $n \in \mathbb{N}^*$: the set of all square matrices of dimension n whose elements can only take the two values 0 and 1.

(ii) $\mathcal{P}_n$, $n \in \mathbb{N}$: the set of permutation matrices of dimension n, that is, those square matrices of dimension n that contain exactly one element equal to 1 per row and per column, their remaining elements being 0. Obviously $\mathcal{P}_n \subset \{0,1\}^{n\times n}$.

(iii) $\mathcal{C}_n$, $n \in \mathbb{N}$: the set of Costas arrays of dimension n.

(iv) Let $A \in \mathcal{P}_n$; if $a_{ij} = 1$, set $f(j) = i$, with $i, j \in \{1,\dots,n\}$. In plain words, $f(j) = i$ expresses the fact that the element of column j that is equal to 1 lies at the ith position of the column. Observe that, since each column has a unique element equal to 1, the others being 0, f is a bijection, hence f^{-1} is a function too: $f^{-1}(i) = j$. Note that f characterizes A unambiguously.

Definition 2.1. Let $A \in \mathcal{P}_n$; then A is a *Costas array* (of *dimension* or *order* n) if and only if the following condition is satisfied: for all $i_1, i_2, i_3, i_4 \in \{1,\dots,n\}$, $i_1 \le i_2$, $i_3 \le i_4$: $(i_1 - i_2, f(i_1) - f(i_2)) = (i_3 - i_4, f(i_3) - f(i_4)) \Rightarrow i_1 = i_2, i_3 = i_4$. In other words, all vectors of the form $(i_1 - i_2, f(i_1) - f(i_2))$, $i_1, i_2 \in \{1,\dots,n\}$, $i_1 < i_2$ are distinct.

This definition can be rephrased to make it easier to visualize and grasp, by collecting vectors together according to their first coordinate. The vectors at hand are as many as the possible choices of $i_1, i_2 \in \{1,\dots,n\}$ with $i_1 < i_2$, that is, $n(n-1)/2$ in total, and, out of these vectors, exactly $n-k$ have their first coordinate equal to k, for $k = 1,\dots,n$ (to be specific, it is those vectors that correspond to $i_1 = i$, $i_2 = i + k$ for $i = 1,\dots,n-k$); these vectors can be collected in a set, say S_k. Within each S_k a vector can be represented only by its second coordinate, as the first is the same for all members of this set.

Consider now two vectors $v_1 \in S_{k_1}$ and $v_2 \in S_{k_2}$. In the context of the definition of a Costas array, we need not worry whether the two vectors are equal if $k_1 \neq k_2$, and if $k_1 = k_2$ we only need to check the second coordinate of the vectors to make sure. So, we can list the second coordinates of the vectors of S_k in a row, and make sure that within this row no number appears twice. If we order the rows one on top of the other, left adjusted or centered, the row corresponding to S_1 being the topmost, and the row corresponding to S_{n-1} being the bottommost, we will obtain a triangular structure: we call this the *difference triangle* of a permutation matrix.

It will also be simpler, at least sometimes, to represent a permutation matrix not as a matrix, but rather by means of its corresponding permutation: if $A \in \mathcal{P}_n$ corresponds to

the function f, its corresponding permutation is $p(A) = f(1)\cdots f(n)$; in other words, we establish a bijection between permutations and permutation matrices, according to which the ith element of the permutation corresponding to a permutation matrix is $f(i)$, the position of the nonzero element of the ith column within this column.

In the following we will not distinguish between A and $p(A)$.

Definition 2.2. Let $A \in \mathcal{P}_n$; the difference triangle of A, T, or $T(A)$, when A needs to appear explicitly, is a triangular structure of $n-1$ rows that has the entries $t_{ij} = f(j) - f(j+i)$, $i = 1,\ldots,n-1$, $j = 1,\ldots,n-i$.

Theorem 2.3. *Let $A \in \mathcal{P}_n$; it is a Costas array if and only if no number appears twice in a row of $T(A)$.*

Proof. It follows from the above discussion that this statement is equivalent to the definition of a Costas array. □

Theorem 2.4. *Let $A \in \mathcal{P}_n$, $n \geq 2$; then $T(A)$ contains exactly $n-i$ elements equal to i in absolute value, $i = 1,\ldots,n-1$.*

Proof. We will use induction.

(i) $n = 2 : p(A)$ contains only one element that equals 1 or -1, hence the statement is true.

(ii) Assume the statement is true for $n \leq s$, and let $n = s+1$; comparing $s+1$ with the remaining elements of $T(A)$ accounts for s entries of $T(A)$; for every $i = 1,\ldots,s$, exactly one of them is in absolute value equal to i; remove $s+1$ from $p(A)$ thus constructing $p(A')$ for some $A' \in \mathcal{P}_s$, whose difference triangle satisfies the proposition to be proved by induction: it contains $s-i$ entries equal to i in absolute value, $i = 1,\ldots,s-1$. Adjoin now, the elements corresponding to $s+1 : T(A)$ will contain $s-i+1 = (s+1)-i$ entries equal to i, $i = 1,\ldots,s-1$, plus one new entry equals to s.

This completes the proof. □

A very useful observation about Costas arrays is the following.

Theorem 2.5. *Let the permutation $P = f(1)\cdots f(n)$, $n \in \mathbb{N}^*$, correspond to a Costas array; then, for any $1 \leq s < t \leq n$, the part $P' = f(s)\cdots f(t)$ of the permutation has the Costas property; if it so happens that the numbers in P' are consecutive integers, that is, that $\{f(i)\}_{i=s}^{t} = \{a, a+1,\ldots,a+t-s-1\}$ for some $a \in \mathbb{N}$, then the permutation $P'' = f(s)-a+1,\ldots,f(t)-a+1$ represents a Costas array of lesser order than P.*

Proof. P' has the Costas property because each row of its difference triangle is a subset of the corresponding row of the difference triangle of P. Moreover, the Costas property depends not on the values of the elements of the permutation, but on their differences only; hence, if P' contains consecutive integers, we can subtract from each of its elements

an integer in order to make the smallest of them equal to 1, without affecting the difference triangle and hence the Costas property; P'', the product of this subtraction, will correspond to a Costas array. □

It will be useful occasionally to think of Costas arrays as permutation matrices whose 0 elements are replaced with nothing, that is, they are left blank, and whose 1 elements are replaced with "dots". We will call this the *dot representation* of a Costas array.

3. History of Costas arrays

Costas arrays arise in sonar and radar applications: both of these devices are used to identify the position and velocity of an object, the target. In order to accomplish this task, they emit pulses at some frequency or frequencies, and they receive the signals that result from the reflection of these pulses on the target. The time difference between emission and reception provides the distance of the target from the device, while the frequency difference between the two, as the Doppler effect stipulates, gives an indication of the speed of the target.

Imagine that we operate our radar or sonar by emitting pulses sequentially at frequencies f_i, $i = 1,\dots,n$, at times t_i, $i = 1,\dots,n$, assumed from now on to be integers between 1 and n, for some n, and by repeating this pattern periodically in time. This technique of varying the emission frequency through time is known as *frequency hopping* and it gives us the opportunity to make our device robust to noise. We will see below that the best results are obtained when no two f_is are equal.

Let us first describe the operation of a device such as the one just described in a noiseless environment: under the assumption that the target moves at a speed that can be considered to be constant throughout the emission cycle of the n pulses, and much less than the propagation speed of the pulses, all pulses will experience almost the same delay and the same frequency shift, so that the set of received pulses will be identical to the set of transmitted pulses, except that it will be shifted in time and frequency. By calculating then the cross-correlation between the transmitted and the received set of pulses we can determine these shifts, and therefore determine the distance and speed of the target.

In order to see this more mathematically, let E be the emitted signal such that $E = \{f(i)\}_{i=-\infty}^{\infty}$, where each $f(i)$ can either be an integer from 1 to n, or a silence X; assume also that the integer values, which model the emission frequencies, appear consecutively; without loss of generality, assume that $f(i) = X$, $i < 1$, $i > n$, so $E = \cdots X f(1) \cdots f(n) X \ldots$. Let also $R = \{f'(i)\}_{i=-\infty}^{\infty}$ denote the received signal. Ideally, in the absence of noise, as we described above, there will be two integers τ and f so that $f'(i) = f(i-\tau) + f$ for all $i \in \mathbb{Z}$, that is, R will be a version of E shifted in time and frequency, due to reflection from the target and its speed. We proceed to calculate $C_{E,R}(v,h) = \sum_{i\in\mathbb{Z}} [f(i) = f'(i+v) - h] = C_{E,E}(v-\tau, f-h)$, $v,h \in \mathbb{Z}$, where we define $X = X$ to be false; at $v = \tau$, $h = f$, $C_{E,R}$ will be maximal, namely $C_{E,R}(\tau, f) = n = C_{E,E}(0,0)$.

We just saw that the autocorrelation of E has a maximum of n at $(0,0) = (n,n)$; but what are the values of $C_{E,E}$ away of this point? In particular, what is the maximum of these values $\max_{(v,h)\neq(0,0)} C_{E,E}(v,h)$? If we consider any two frequencies $f(i)$ and $f(j)$ not

equal to X, by choosing $v = i - j$ and $f = f(j) - f(i)$, we can bring them to coincide, so it is always the case that $\max_{(v,h)\neq(0,0)} C_{E,E}(v,h) \geq 1$.

What happens though when noise is present? Assuming that the noise is going to affect both time and frequency, by introducing time delays and frequency shifts, it will prevent R from completely matching E, so that $C_{E,R}(\tau, f) < n$ in general. It is now that the exact pattern used for E becomes crucial: if the maximum of E is not unique and well pronounced, we risk computing wrong τ and f, thus calculating wrong distances and speeds, and maybe even spurious targets. The solution to this is to make the maximum of the autocorrelation of E as pronounced as possible, by keeping all other values as low as possible. The best we can do then is to arrange things so that $\max_{(v,h)\neq(0,0)} C_{E,E}(v,h) = 1$, that is, whenever we choose v and h so that two frequencies coincide, none of the remaining ones will. But this is precisely the definition of the Costas array!

Finally, if $f(i) = f(j)$, for $i < j$, a simple time delay will result in a positive autocorrelation for $v = i - j$. As time delays are in practice very frequent, this would be most undesirable. Hence, no two $f(i)$s should be equal. Another way to express that is that energy should be maximized for any given time and frequency to facilitate detection, which means that at a given time no more than one frequency should be used, and that a given frequency should not be used more than once.

The preceding explanation for the creation of Costas arrays is a (quite liberal) adaptation of the ideas of Costas [5, 6], the inventor of these arrays, whose name they bear. Costas was able to find by hand examples of Costas arrays up to order 12 [18]; unable to find one of size 13, he contacted Prof. Golomb, who provided construction algorithms based on the theory of finite fields [9, 12], which we will analyze a bit later.

4. Some counting results on Costas arrays

Even before any explicit construction of Costas arrays takes place, the definition itself allows us to derive and state some interesting properties.

4.1. Symmetry

Theorem 4.1. *Let $A \in \mathcal{C}_n$, for $n \in \mathbb{N}^*$; if $A = A^T$, 3 more Costas arrays can be constructed, so that all 4 are distinct; if $A \neq A^T$, 7 more Costas arrays can be constructed, so that all 8 are distinct. The sets of Costas arrays so constructed are disjoint; hence, Costas arrays come in sets of 4 or 8.*

Proof. We can carry out the proof by thinking of Costas arrays either as arrays or permutations.

(i) We can flip a Costas array vertically, and this clearly does not affect its Costas property, as the only result of the flip on the vectors between nonzero elements is to change the sign of their second coordinate; equivalently, from the permutation $f(1)\cdots f(n)$ we produce $n+1-f(1),\ldots,n+1-f(n)$, whose difference triangle is the same as of the original, but with opposite entry signs.

(ii) We can flip a Costas array horizontally, and this clearly does not affect its Costas property, as the only result of the flip on the vectors between nonzero elements is to change the sign of their first coordinate; equivalently, from the permutation $f(1)\cdots f(n)$

we produce $f(n)\cdots f(1)$, whose difference triangle is the same as of the original, but with opposite entry signs, and horizontally flipped rows.

(iii) We can flip the array around its main diagonal; the resulting matrix will be different if the original is not symmetric, but the Costas property is not affected, as the only result of the flip on the vectors between nonzero elements is to swap the coordinates.

Let us denote the three flips by V, H, T, respectively. In algebraic terms, they generate a group, whose constraining relations are $V^2 = H^2 = T^2 = I$ (I is the identity), and that $V = THT$. This is the group of symmetries of the square, which has 8 elements that can be denoted by I, V, H, VH, T, VT, HT, VHT. Define now $S(A) = \{A,\ VA,\ HA,\ VHA,\ TA,\ VTA,\ HTA,\ VHTA\}$, which has 8 elements, or 4 if $A = TA$; this is the orbit of A under the action of the group, and we know by algebra that two orbits either coincide or are disjoint. Equivalently, the relation $A \sim B \Leftrightarrow B \in S(A)$ is an equivalence relation, which divides $\mathcal{C}_n$ into the equivalence classes $S(A)$, $A \in \mathcal{C}_n$, among which any two either coincide or are disjoint. □

4.2. Density. A rather weak result about the density of Costas arrays appears in [13].

Theorem 4.2. *$|\mathcal{C}_n|/n! \to 0$; the density of the Costas arrays tends to 0.*

Proof. The proof is rather long but has a very clear structure. It will be presented in steps.

(1) Let us consider the permutation $P = f(1)\cdots f(n)$, $n \in \mathbb{N}^*$, and let us consider the points $(i, f(i))$, $i = 1,\ldots,n$, on the plane. If three of them lie equally spaced on a line, P does not correspond to a Costas array; let us call such a configuration of three of the above points lying equally spaced on a line an L_3 configuration.

(2) The probability for a permutation of order n to be a Costas array is by definition $|\mathcal{C}_n|/n!$. Let X be the random variable denoting the number of L_3 configurations in P, and suppose its mean is μ and its variance is σ^2. Then

$$\frac{|\mathcal{C}_n|}{n!} = \mathbb{P}(P \text{ is Costas}) \le \mathbb{P}(X = 0) \le \mathbb{P}\big(|X-\mu| \ge \mu\big) \le \frac{\sigma^2}{\mu^2}. \tag{4.1}$$

The last equality follows by the application of Chebychev's inequality. So, all that is needed now is the computation of μ and σ^2.

(3) How many L_3 configurations can a permutation of order n contain? We only need to count the number l_n of different ways in which we can choose its endpoints, as then its midpoint is uniquely defined. Suppose then the endpoints are $(i, f(i) = j)$ and $(i', f(i') = j')$; following the square bracket notation, according to which $[Q]$ is 1 if Q is true and 0 if it is false, and using $x \mid y$ to denote that x divides y, we can write

$$\begin{aligned} l_n &= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{i'=1}^{n}\sum_{j'=1}^{n}[2 \mid i-i'][2 \mid j-j'][i<i'][j \ne j'] \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{i'=1}^{n}\sum_{j'=1}^{n}\sum_{k}\sum_{k'}[i' = 2k+i][j' = 2k'+j][i<i'][j \ne j'] \end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k>0}\sum_{k'\neq 0}[1 \le 2k+i \le n][1 \le 2k'+j \le n] \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k>0}\sum_{k'\neq 0}[1 \le 2k+i < n+1][1 \le 2k'+j < n+1] \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k>0}\sum_{k'\neq 0}\left[\frac{1-i}{2} \le k < \frac{n+1-i}{2}\right]\left[\frac{1-j}{2} \le k' < \frac{n+1-j}{2}\right] \\
&= \sum_{i=1}^{n}\left(\left\lceil\frac{n+1-i}{2}\right\rceil - 1\right)\sum_{j=1}^{n}\left(\left\lceil\frac{n+1-j}{2}\right\rceil - \left\lceil\frac{1-j}{2}\right\rceil - 1\right).
\end{aligned}
\tag{4.2}
$$

The final formula can be further simplified into

$$
l_n = \sum_{i=1}^{n}\left(\left\lceil\frac{i}{2}\right\rceil - 1\right)\sum_{j=1}^{n}\left(\left\lceil\frac{n+1-j}{2}\right\rceil - \left\lceil\frac{1-j}{2}\right\rceil - 1\right). \tag{4.3}
$$

In order to advance further we need to distinguish cases according to whether n is even or odd.

(i) If $n = 2m+1$ for $m \in \mathbb{N}$ we get

$$
\begin{aligned}
l_n &= \sum_{i=1}^{2m+1}\left(\left\lceil\frac{i}{2}\right\rceil - 1\right)\sum_{j=1}^{2m+1}\left(m + \left\lceil -\frac{j}{2}\right\rceil - \left\lceil\frac{1-j}{2}\right\rceil\right) \\
&= \sum_{i=1}^{2m+1}\left(\left\lceil\frac{i}{2}\right\rceil - 1\right)\sum_{j=1}^{2m+1}\left(m - \left\lfloor\frac{j}{2}\right\rfloor + \left\lfloor\frac{j-1}{2}\right\rfloor\right) \\
&= [2(0+1+\cdots+m-1)+m][(2m+1)m-m] \\
&= 2m^2[m+m(m-1)] = 2m^4 = \frac{(n-1)^4}{8}.
\end{aligned}
\tag{4.4}
$$

(ii) If $n = 2m$ for $m \in \mathbb{N}$ we get

$$
\begin{aligned}
l_n &= \sum_{i=1}^{2m}\left(\left\lceil\frac{i}{2}\right\rceil - 1\right)\sum_{j=1}^{2m}\left(m - 1 + \left\lceil\frac{1-j}{2}\right\rceil - \left\lceil\frac{1-j}{2}\right\rceil\right) \\
&= \sum_{i=1}^{2m}\left(\left\lceil\frac{i}{2}\right\rceil - 1\right)\sum_{j=1}^{2m}(m-1) \\
&= 2(0+1+\cdots+m-1)2m(m-1) = m(m-1)2m(m-1) \\
&= 2m^2(m-1)^2 = \frac{n^2(n-2)^2}{8}.
\end{aligned}
\tag{4.5}
$$

(4) Now we are ready to compute μ and σ. By $L_3 \subset P$ we denote the fact that the particular L_3 configuration appears in P. For $n \geq 3$,

$$\mu = \frac{1}{n!}\sum_{P\in\mathcal{P}_n} X(P) = \frac{1}{n!}\sum_{P\in\mathcal{P}_n}\sum_{L_3\subset P} 1 = \frac{1}{n!}\sum_{L_3}\sum_{\{P\in\mathcal{P}_n \mid P\supset L_3\}} 1 = \frac{1}{n!}\sum_{L_3}(n-3)! = \frac{l_n}{n(n-1)(n-2)}, \tag{4.6}$$

whence we get that $\mu \approx n/8$:

$$\begin{aligned}\mathbb{E}(X^2) &= \frac{1}{n!}\sum_{P\in\mathcal{P}_n}\big(X(P)\big)^2 = \frac{1}{n!}\sum_{P\in\mathcal{P}_n}\left(\sum_{L_3\subset P} 1\right)^2 \\ &= \frac{1}{n!}\sum_{P\in\mathcal{P}_n}\sum_{(L_3,L_3')\subset P} 1 = \frac{1}{n!}\sum_{(L_3,L_3')}\sum_{\{P\in\mathcal{P}_n \mid P\supset(L_3,L_3')\}} 1 \\ &= \frac{1}{n!}\big[m_3(n-3)! + m_2(n-4)! + m_1(n-5)! + m_0(n-6)!\big].\end{aligned} \tag{4.7}$$

The notation $(L_3, L_3') \subset P$ stands for the fact that the configurations L_3 and L_3' belong both to P, their order being important. m_i, $i = 3, 2, 1, 0$, in the formula stands for the number of ordered pairs of L_3 configurations which have precisely i points in common; we proceed now to find their values, or at least estimates of them.

(i) $m_3 = l_n$.

(ii) $m_2 \leq 4l_n$, as two L_3 configurations can intersect in two points in exactly 4 ways. If we denote the 2 configurations by 123 and 1'2'3', and we denote their common points by X, the 4 possible intersections at question are $1XX3'$, $1'XX3$, $X2X3'$, and $X2'X3$.

(iii) In order to estimate m_1, we think as follows: we can pick L_3 in l_n ways, and the point in common of the two in 3 ways. If this common point is an endpoint of L_3', we can choose its other endpoint, and therefore L_3', in $n^2/4$ ways at most (as both the horizontal and the vertical distance between the endpoints need to be even); if the common point is the midpoint of L_3', we can choose an endpoint, and hence L_3', in at most $n^2/2$ ways. Hence $m_1 \leq 3l_n(n^2/2 + n^2/4) = (9/4)n^2 l_n$.

(iv) Finally, $m_0 \leq l_n^2$.

To sum up,

$$\begin{aligned}\mathbb{E}(X^2) &\leq \frac{1}{n!}\left[l_n(n-3)! + 4l_n(n-4)! + \frac{9}{4}n^2 l_n(n-5)! + l_n^2(n-6)!\right] \\ &\leq \mu\left[1 + \frac{4}{n-3} + \frac{9n^2}{4(n-3)(n-4)}\right] + \frac{l_n^2}{n(n-1)(n-2)(n-3)(n-4)(n-5)} \\ &\leq 5\mu + \frac{l_n^2}{n(n-1)(n-2)(n-3)(n-4)(n-5)}\end{aligned} \tag{4.8}$$

for n sufficiently large.

Therefore,

$$\sigma^2 = \mathbb{E}(X^2) - \mu^2 \le 5\mu + \frac{l_n^2}{n(n-1)(n-2)(n-3)(n-4)(n-5)} - \frac{l_n^2}{n^2(n-1)^2(n-2)^2}$$
$$= 5\mu + \left[\frac{n(n-1)(n-2)}{(n-3)(n-4)(n-5)} - 1\right]\mu^2. \tag{4.9}$$

(5)

$$\frac{|\mathscr{C}_n|}{n!} \le \frac{\sigma^2}{\mu^2} \le \frac{5}{\mu} + \frac{9n^2 - 45n + 60}{(n-3)(n-4)(n-5)} \le \frac{C}{n} \tag{4.10}$$

for sufficiently large n, and therefore the statement holds. □

The finishing sentence of [13] is that "it would be interesting to have better bounds on $[\mathscr{C}_n]$, but this will require more sophisticated arguments than [those] used here." Indeed, a more sophisticated argument was used later in [20], and produced a formula for the probability $p_n = |\mathscr{C}_n|/n!$; in contrast to the formula in [13], though, this one is partly heuristic, as its final form results from an "educated guess," and it contains an unspecified parameter that needs to be be evaluated through fitting to the actual probabilities computed (and available for $n \le 25$ today [1]). It is worth taking a detailed look at it, as the argument it is based upon is rather important, while the original paper [20], due to its brevity, offers no detailed proof neither of the argument nor of the formula.

Theorem 4.3. *Let $P \in \mathscr{P}_n$, $n \in \mathbb{N}^*$; if the first $k < n-1$ rows of $T(P)$ are free of repetitions, then no repetitions on row $k+1$ can be closer than k places apart.*

Proof. Let $P = f(1)\cdots f(n)$, and suppose that $\exists 1 \le i_1 < i_2 < i_3 < i_4 \le n$ so that $f(i_1) - f(i_3) = f(i_2) - f(i_4)$ and $i_3 - i_1 = i_4 - i_2 = k+1$, while $i_2 - i_1 = s < k$. It follows that $i_4 - i_3 = i_2 - i_1 = s$ and $f(i_1) - f(i_2) = f(i_3) - f(i_4)$ as well, which implies that a repetition exists on a previous row, contrary to our hypothesis. Therefore, $s \ge k$ and the proof is complete. □

This is a very important result, because it reduces the number of pairs of the elements of the difference triangle we need to check in order to assert that a particular permutation corresponds to a Costas array. The proof offered above is an adaptation of the original proof [4].

Theorem 4.4. *The total number of pairs of $T(P)$, with $P \in \mathscr{P}_n$, $n \in \mathbb{N}^*$, that needs to be checked in order to ascertain that $P \in \mathscr{C}_n$ is*

(i) $TP(n) = n(n-1)(n-2)/6$, *if Theorem 4.3 is not taken into account,*
(ii) (1) $IP(n) = n(n-2)(2n+1)/24$, *n even,*
(2) $IP(n) = (n+1)(n-1)(2n-3)/24$, *$n$ odd,*
if it is.

TP stands for total pairs, and IP for independent pairs.

Proof. Row i of the difference triangle has $n-i$ elements, $i = 1,\ldots,n-2$, hence the total number of pairs per row is $(n-i)(n-i-1)/2$, and the total number of pairs that needs to

be checked is $\sum_{i=1}^{n-2}(n-i)(n-i-1)/2 = \sum_{i=1}^{n-2}(i+1)i/2 = \sum_{i=0}^{n-2}(i+1)i/2 = 1/2\sum_{0}^{n-1}(i+1)^{\underline{2}} = (i+1)^{\underline{3}}/6\,|_0^{n-1} = n(n-1)(n-2)/6$.

If, on the other hand, we take Theorem 4.3 into account, we actually need to check less pairs: checking element 1 of row i will require comparing it to all elements at $i+1,\ldots,n-i$, as the elements at $2,\ldots,i$ are certainly different from it; similarly, element j of row i will be compared only to $i+j,\ldots,n-i$, $i=1,\ldots,n$, $j=1,\ldots,n-2i$. In total then, row i will require $\sum_{j=1}^{n-2i}(n-2i-j+1) = \sum_{j=1}^{n-2i} j = (n-2i)(n-2i+1)/2$ checks, hence the total number of checks for all rows will be $\sum_{i=1}^{n-2}\max((n-2i)(n-2i+1)/2,0) = 1/2\sum_{i=1}^{\lfloor n/2\rfloor}(n-2i)(n-2i+1)$.

(i) For $n=2m$, $m\in\mathbb{N}^*$, this becomes $\sum_{i=1}^{m}(m-i)(2m-2i+1) = \sum_{i=0}^{m-1} i(2i+1) = \sum_{i=0}^{m-1} i + 2\sum_{i=0}^{m-1} i^2 = m(m-1)/2 + 2m(m-1)(2m-1)/6 = m(m-1)(4m+1)/6 = n(n-2)(2n+1)/24$.

(ii) For $n=2m+1$, $m\in\mathbb{N}^*$, this becomes $\sum_{i=1}^{m}(m-i+1)(2m-2i+1) = \sum_{i=0}^{m-1}(i+1)(2i+1) = 3\sum_{i=0}^{m-1} i + 2\sum_{i=0}^{m-1} i^2 + m = 3m(m-1)/2 + 2m(m-1)(2m-1)/6 + m = m(m-1)(4m-1)/6 = (n+1)(n-1)(2n-3)/24$.

This completes the proof. □

We proceed now to make the simplifying assumption that all independent (in the sense of the previous theorem) pairs of entries in the rows of $T(P)$ are actually independent, that is, that the entries of one are independent of the entries of the others; we can assume then that the entries of such a pair will be equal with probability $\overline{P}_R(n)$, and therefore that the expression $p_n = (1-\overline{P}_R(n))^{IP(n)}$ approximates the probability that a permutation is a Costas array. Namely, we expect that

$$\frac{|\mathcal{C}_n|}{n!} \approx \left(1-\overline{P}_R(n)\right)^{IP(n)}. \tag{4.11}$$

We still need to find $\overline{P}_R(n)$. Let us assume that the pair we are looking at contains the two entries A and B. We can work as follows:

$$\overline{P}_R(n) = \mathbb{P}(A=B) = \mathbb{P}\left(|A|=|B|\right)\mathbb{P}\left(AB>0 \mid |A|=|B|\right). \tag{4.12}$$

According to Theorem 2.4, $T(P)$ will contain $n-i$ entries of i in absolute value, $i=1,\ldots,n-1$. If we want both entries to equal i, we will be able to choose them in $(1/2)(n-i)(n-i-1)$ ways, while the total number of ways we could choose them is $(1/2)(n(n-1)/2)((n(n-1)/2)-1)$. Hence

$$\begin{aligned}\mathbb{P}\left(|A|=|B|\right) &= \sum_{i=1}^{n-1}\mathbb{P}\left(|A|=|B|=i\right) = \sum_{i=1}^{n-1}\frac{(n-i)(n-i-1)}{\left(n(n-1)/2\right)\left(\left(n(n-1)/2\right)-1\right)} \\ &= \frac{n(n-1)(n-2)/6}{\left(n(n-1)/2\right)\left(n(n-1)/2-1\right)} = \frac{2}{3(n+1)}.\end{aligned} \tag{4.13}$$

$\mathbb{P}(AB>0\,|\,|A|=|B|)$ is the probability that A and B are of the same sign given they are equal in absolute value. We will assume that this is a constant (independent of n)

probability p. Then, the formula becomes

$$\frac{|\mathscr{C}_n|}{n!} \approx \left(1 - \frac{K}{n+1}\right)^{IP(n)}, \quad K = \frac{2p}{3}. \tag{4.14}$$

In [20] K is treated as a simple proportionality constant, not connected to any other quantities, and it gets determined by fitting the equation to the known values of the probability that a permutation of order n has the Costas property. At the time, this was known for $n \leq 17$, but later the experiment was repeated for $n \leq 25$ (see [1]): in all cases the fitting process gives $K \approx 1.1$, which clearly violates the assumption that $p = (3/2)K$ is a probability; nevertheless, this formula remains a valuable tool, as the fitting is remarkably successful, and as it is still the best estimate of the Costas array probability we have.

5. Currently known results

All proofs for the existence of Costas arrays hitherto presented are

(i) *constructive*: existence is shown by explicit construction or a construction algorithm;

(ii) *dimension specific*: it has been shown that $\mathscr{C}_n \neq \varnothing$ for n in a *genuine* subset of $\mathbb{N}^*$.

The Costas arrays we know of today have been generated by one of the following methods.

(1) Exhaustive search of $\mathscr{P}_n$: it has yielded all Costas arrays up to $n \leq 26$ [1, 2, 19].

(2) Construction algorithms: they produce Costas arrays of dimensions equal to or a bit less than primes or powers of primes [9, 12].

(3) A trial and error approach presented in [18] which yielded 4 previously unknown Costas arrays.

Let us review these three methods one by one.

6. Exhaustive search

The method of exhaustive search is straightforward: for a given $n \in \mathbb{N}^*$, we examine every $A \in \mathscr{P}_n$ and decide whether or not it is a Costas array; thus, we get all Costas arrays of order n. The computational complexity of the method is of the order $n^3 n!$: there are $n!$ permutations of order n, and testing each one requires $n(n-1)/2$ subtractions (to find the difference between all possible pairs of elements of the permutation), and then $\sum_{k=1}^{n-1} k(k-1)/2 = n(n-1)(n-2)/6$ comparisons (all pairs of elements within a row of the difference triangle, for each row).

The situation can be improved considerably by recognizing that

(1) the symmetry explained in Section 4.1 reduces the number of necessary tests ideally by 8;

(2) not all of the difference triangle needs to be computed in most cases: at the very least, we can use Theorem 4.3; at best, once a repetition is detected, there is no reason to continue working on that specific permutation;

(3) permutations share parts of their difference triangles.

Table 6.1. Number of Costas arrays per order found by exhaustive search.

Order	Number	Order	Number	Order	Number
1	1	10	2160	19	10240
2	2	11	4368	20	6464
3	4	12	7852	21	3536
4	12	13	12828	22	2052
5	40	14	12752	23	872
6	116	15	19612	24	200
7	200	16	21104	25	88
8	444	17	18276	26	56
9	760	18	15096	27	?

Whether one is able to incorporate all of these improvements in one's code is, of course, a different matter. The best exhaustive search results available today are due to the efforts of J. K. Beard and his associates, who used code written in assembly and parallel programming techniques over a Beowulf cluster, raising the dimension for which all Costas arrays have been tabulated to 26 [1, 2, 19]. Regarding 26 in particular, the computation was completed independently by two groups, namely Beard's and Rickard's, although it is clear that the former group finished earlier; their results were identical [19].

The reports of Beard's group mention nothing about the difficulty of their task; the author of this paper, wanting to get a first hand experience of the difficulty involved, wrote a program in Java and ran it on an Acer Aspire 1714SMi laptop (with an Intel Pentium 4 3.4 GHz processor and 1 GB of RAM): the search for Costas arrays of order 16 took about a day to complete.

The total number of Costas arrays for orders up to and including 26 are shown in Table 6.1.

7. Construction algorithms

There are essentially two construction algorithms: the *Welch construction* and the *Golomb construction*. Both of them admit several variations/modifications that increase the number of Costas arrays they can construct; and both of them are based on the theory of finite (Galois) fields, which we are going to review before embarking on the relevant theorems and proofs.

The constructions will be labeled in the form letter/number, where the letter denotes the category of the construction (W for Welch, G for Golomb, L for Lempel, and T for Taylor), while the number denotes how much smaller the order of the Costas array is compared to the size of the finite field used in its construction (all these concepts will be clarified below). This nomenclature of the construction algorithms is the same as the one used in [1, 12].

7.1. Elements of Galois (finite) fields

7.1.1. The modulo function

Definition 7.1. Let $x \in \mathbb{Z}$, $y \in \mathbb{N}^*$. Then, x modulo y, $x \bmod y$, is defined to be the unique $r \in \mathbb{N}$ that satisfies the following conditions:

(1) $\exists m \in \mathbb{Z} : x = ym + r$,
(2) $0 \le r < y$.

An immediate consequence of the definition is that for all $k \in \mathbb{Z} : (x + ky) \bmod y = x \bmod y$.

Theorem 7.2. *For all* $u, v \in \mathbb{Z}$, $y \in \mathbb{N}^*$,

(1) $(u + v) \bmod y = (u \bmod y + v \bmod y) \bmod y$,
(2) $(uv) \bmod y = ((u \bmod y)(v \bmod y)) \bmod y$.

Proof. Let $u \bmod y = r_u$ and $v \bmod y = r_v$, that is, $u = m_u y + r_u$, $u = m_v y + r_v$ for some $m_u, m_v \in \mathbb{Z}$:

(1) $(u + v) \bmod y = (m_u y + r_u + m_v y + r_v) \bmod y = (r_u + r_v) \bmod y$ and the proof is complete;
(2) $(uv) \bmod y = ((m_u y + r_u)(m_v y + r_v)) \bmod y = (r_u r_v + y(m_u m_v y + m_u r_v + m_v r_u)) \bmod y = (r_u r_v) \bmod y$ and the proof is complete. □

We will occasionally use different symbols for addition and multiplication modulo n than for their usual counterparts, so we can tell them easily apart: $x \oplus y = (x + y) \bmod n$, $x \ominus y = (x - y) \bmod n$, and $x \odot y = (xy) \bmod n$; n will always be clear from the context.

7.1.2. Definition of a field

Definition 7.3. Let S be a set, and let two functions $\oplus : S \times S \to S$ and $\odot : S \times S \to S$ be defined on it. Then S will be called a *field* if and only if the following conditions hold:

(1) S is a *commutative group* with respect to $\oplus$:
  (a) for all $x, y \in S$, $x \oplus y = y \oplus x$ (commutativity),
  (b) for all $x, y, z \in S$, $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ (associativity),
  (c) $\exists 0 \in S$: for all $x \in S$ $x \oplus 0 = x$ (neutral element of addition),
  (d) for all $x \in S$ $\exists (-x) \in S : x \oplus (-x) = 0$ (negative element);
(2) $S - \{0\}$ is a *commutative group* with respect to $\odot$:
  (a) for all $x, y \in S$, $x \odot y = y \odot x$ (commutativity),
  (b) for all $x, y, z \in S$, $x \odot (y \odot z) = (x \odot y) \odot z$ (associativity),
  (c) $\exists 1 \in S$: for all $x \in S$ $x \odot 1 = x$ (neutral element of multiplication),
  (d) for all $x \in S - \{0\} \exists x^{-1} \in S : x \odot x^{-1} = 1$ (inverse element);
(3) for all $x, y, z \in S : x \odot (y \oplus z) = x \odot y \oplus x \odot z$ (distributivity);

S is an *additive group*; $S - \{0\}$ is a *multiplicative group*.

In plain words, a field is a set in which addition and multiplication are not only defined, but also have the same familiar properties they have in $\mathbb{R}$, the set (field) of the real

numbers. A useful observation is this: by plugging $y = z = 0$ in the distributivity formula, since $0 \oplus 0 = 0$, we obtain for all $x \in S$, $0 \odot x = 0$.

From now on we will follow the familiar convention when there is no danger of confusion: drop $\odot$ completely, $x \odot y = xy$, and write $x \oplus y$ as $x + y$; we also use powers normally: $x \odot x = x^2$, and so forth.

Notice that we avoided calling the elements of finite fields "numbers"; we will see why a bit later.

7.1.3. Properties of fields

THEOREM 7.4. *0 and 1 are unique.*

Proof. Suppose there are two neutral elements for addition, 0 and 0'; then $0 + 0' = 0$, as $0'$ is neutral, and $0 + 0' = 0'$, as 0 is neutral; hence $0 = 0'$. Similarly, $1 \cdot 1' = 1 = 1'$. □

THEOREM 7.5 (cancellation law). $xy = 0 \Rightarrow x = 0 \vee y = 0$.

Proof. Suppose $x \neq 0$; then x^{-1} exists, and $x^{-1}(xy) = x^{-1}0 = 0 = (x^{-1}x)y = 1y = y \Rightarrow y = 0$. □

7.1.4. A family of finite fields

Definition 7.6. A field S is *finite* if and only if it has a finite number of elements: $|S| < \infty$.

Definition 7.7. Define $\mathbb{F}_n$, $n \in \mathbb{N}^*$, $n \geq 2$, to be the set $\{0, 1, \ldots, n-1\}$, and define on it addition and multiplication in the usual way as in $\mathbb{R}$, but modulo n.

THEOREM 7.8. *Consider $\mathbb{F}_n$, $n \in \mathbb{N}^*$, $n \geq 2$; it is a field if and only if $n = p$, where p is a prime number.*

Proof. We need to check the defining properties of a field, but associativity, commutativity, and distributivity follow by the usual definition of addition and multiplication in $\mathbb{R}$ and Theorem 7.2; moreover, 0 and 1 keep their roles as neutral elements, again by Theorem 7.2; and, finally, by the same theorem, $x + y = 0 \Rightarrow x \oplus y = 0$, so that the existence of the negative element for all $x \in \mathbb{F}_n$ is guaranteed.

It is the existence of the multiplicative inverses that requires some attention; we will prove that they exist when n is a prime, and that they do not (always) exist when it is not.

(1) Let $n = pq$, with $p, q \in \mathbb{F}_n$. Then, $(pq) \bmod n = p \odot q = n \bmod n = 0$, so that the product of two nonzero elements of $\mathbb{F}_n$ is 0, contradicting Theorem 7.5, and therefore $\mathbb{F}_n$ is not a field.

(2) Let n be a prime p: $n = p$. Then, consider $x \in \mathbb{F}_n$, $x \neq 0$, and consider the numbers $(ix) \bmod p = i \odot x$, $i = 1, \ldots, p-1$. No two of them are equal, for if $i \odot x = j \odot x$, it follows that $(i - j) \odot x = 0$, so that p divides either $i - j$ or x; but $0 < x < p$ and $0 < |i - j| < p$, so that both alternatives are impossible. For the same reason, none of these numbers is 0.

It follows that the numbers $i \odot x$, $i = 1, \ldots, p-1$, correspond bijectively to the numbers $1, \ldots, p-1$; in particular, there exists an $i \in \mathbb{F}_n$: $i \odot x = 1 \Rightarrow i = x^{-1}$, and the proof is complete. □

7.1.5. Fermat's little theorem

THEOREM 7.9 (Fermat's little theorem). *Let $x \in \mathbb{F}_p$, $x > 1$, with p prime. Then,* $(x^{p-1}) \bmod p = 1$.

Proof. Consider the numbers $(ix) \bmod p = i \odot x$, $i = 1, \ldots, p-1$; as in the proof of Theorem 7.8, we can demonstrate that they are all nonzero and distinct, and, hence, that there is a bijection between them and the numbers $1, \ldots, p-1$. It follows that $[(1 \odot x)(2 \odot x) \cdots ((p-1) \odot x)] = (p-1)! \Rightarrow (1x2x \cdots (p-1)x) \bmod p = [(p-1)!] \bmod p = [(p-1)! x^{p-1}] \bmod p \Rightarrow [(p-1)!(x^{p-1} - 1)] \bmod p = 0$. This implies that p divides either $(p-1)!$, which is impossible, or $x^{p-1} - 1$, which is necessarily true. Hence, $(x^{p-1}) \bmod p = 1$, and the proof is complete. □

7.1.6. Primitive roots of finite fields. Theorem 7.9 does *not* prove that $p-1$ is the least positive integer with this property: it may still be the case that for a particular x $\exists 0 < a < p-1$ so that $x^a \bmod p = 1$. Divide $p-1$ by a : $p - 1 = ma + r$ for some $m \in \mathbb{N}$ and $0 \le r < a$. But then $x^r \bmod p = x^{p-1-ma} \bmod p = (x^{p-1} \bmod p) \odot (x^a \bmod p)^{-m} \bmod p = 1 \odot 1^m = 1$; if $r > 0$ we obtain a contradiction, since a was assumed to be the least positive integer with this property, and now we proved that r has it too; therefore, the only alternative is that $r = 0$. We have just proved.

THEOREM 7.10. *Let $x \in \mathbb{F}_p$, $x > 1$, with p prime. Then, for all $x \in \mathbb{F}_p - \{0\}$, there exists a smallest positive integer $a(x)$ for which $x^{a(x)} \bmod p = 1$; also, $a(x)$ divides $p-1$.*

Definition 7.11. A multiplicative group C is *cyclic* if and only if $\exists x \in C : C = \{1, x, x^2, \ldots, x^{n-1}\}$, with $|C| = n \in \mathbb{N}^*$.

Definition 7.12. Let $\mathbb{F}$ be a finite field; $x \in \mathbb{F}$ is called a *primitive root* of $\mathbb{F}$ if $\mathbb{F} = \{0, 1, x, \ldots, x^{n-2}\}$, with $|\mathbb{F}| = n \in \mathbb{N}^*$; in other words, x is a primitive root of $\mathbb{F}$ if and only if the cyclic group of x equals the multiplicative group of $\mathbb{F}$.

In the context of Theorem 7.10, x will be a primitive root of $\mathbb{F}_p$, p prime, if and only if $a(x) = p-1$. But at this point it is not even clear that finite fields have primitive roots. This is indeed the case, as the following theorem demonstrates.

THEOREM 7.13. *Any finite field $\mathbb{F}$ has primitive roots, that is, its multiplicative group is cyclic.*

Proof. Let $y \in \mathbb{F}$, $n = |\mathbb{F}|$, and consider all polynomials of the form $y^r - 1$ with $0 < r \le n - 1$. Consider now a specific $y \in \mathbb{F}$ and consider the cyclic multiplicative group it produces: $C(y) = \{y^i \mid i \in \mathbb{N}\}$. $C(y)$ can of course have at most $n-1$ elements, as many as the nonzero elements of the field are. Hence, as we start forming the powers $y^0, y^1, y^2, \ldots$, according to the multiplication law of the field, we will necessarily find two powers $r_1 < r_2$ for which $y^{r_1} = y^{r_2} \Rightarrow y^{r_2 - r_1} = 1$. Therefore, for every $y \in \mathbb{F} - \{0\}$ there exists a smallest positive $r(y)$ for which $y^{r(y)} = 1$.

Set now $r = \max\{r(y) \mid y \in \mathbb{F} - \{0\}\}$. Then

(i) as all cyclic groups are contained in the multiplicative group of the field, it follows that $r \le n - 1$;

(ii) if $\exists z \in \mathbb{F}$ that does not satisfy $z^r = 1$, but rather $z^{r'} = 1$, with $r' < r$, there are two possibilities:

(1) either r' divides r, in which case $z^r = (z^{r'})^{r/r'} = 1^{r/r'} = 1$, a contradiction,

(2) or it does not. Consider then $yz \in \mathbb{F}$; what is the smallest positive q for which $(yz)^q = 1$? Since $y^q z^q = (yz)^q$, then q must be a multiple of r and r', so the smallest possible value of q is the least common multiple of r' and r, which is strictly larger than r, as we assumed that r' does not divide r. Therefore we get a contradiction, because we chose r to be maximal.

The only alternative then is that for all $y \in \mathbb{F} - \{0\}$, $y^r = 1$, which means that for all $y \in \mathbb{F} - \{0\}$ the polynomial $Y^r - 1$ is divisible by $Y - y$. It follows that the degree of $Y^r - 1$, that is, r, is at least $n - 1 : r \geq n - 1$.

Combining the two results we get that $\exists y \in \mathbb{F} : y^{n-1} = 1$ and $y^i \neq 1, 0 < i < n - 1$, so that the multiplicative group of the field is cyclic. □

This theorem proves an important result, but not in the best possible way, for it gives us no information at all about how to find the primitive roots of a field. This is indeed a difficult problem, and efforts towards its solution [14, 15, 22, 24] were partly associated with the work on Costas arrays. Still, the best approach is to test some elements until we find one; we include an example a bit later. It should be noted, though, that which primitive root we use to express the finite field is not important: if x and y are two primitive roots of $\mathbb{F}$, which has n elements, we can write $\mathbb{F} = \{0, 1, x, \ldots, x^{n-2}\} = \{0, 1, y, \ldots, y^{n-2}\}$, and the bijection $f(x^i) = y^i$, $i = 0, \ldots, n - 2$, $f(0) = 0$, with the property that $f(x^i x^j) = f(x^i) f(x^j)$ is an isomorphism, hence the two representations of the field are the same.

How many primitive roots does a field $\mathbb{F}$ have? A quite simple argument allows us to establish their number, as well as to provide an "algorithm" for their determination, which suffers from the slight defect that we need one of them to determine all the others.

Definition 7.14. Let $n \in \mathbb{N}$; the *Euler function* $\phi(n)$ denotes how many numbers in $1, \ldots, n$ have no common factor with n.

Theorem 7.15. *Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = n \in \mathbb{N}^*$; then the number of primitive roots it has is $\phi(n - 1)$. Moreover, if $f \in \mathbb{F}$, is a primitive root, then f^i, $i = 2, \ldots, n - 2$, is also a primitive root if and only if i has no common factor with $n - 1$.*

Proof. According to Theorem 7.13, $\mathbb{F}$ has at least one primitive root f, so that all of the nonzero elements of $\mathbb{F}$ can be expressed by means of its powers: $\mathbb{F} = \{0, 1, f, \ldots, f^{n-2}\}$. Consider now the element f^i, $i = 2, \ldots, n - 2$; it will also be a primitive root if and only if the powers $(f^i)^j = f^{ij}$, $j = 0, \ldots, n - 2$, span all the nonzero elements of $\mathbb{F}$; notice that $(f^i)^0 = f^0 = 1$ and that $(f^i)^{n-1} = f^{i(n-1)} = (f^{n-1})^i = 1^i = 1$.

As these powers are already as many as the nonzero elements of $\mathbb{F}$, it is enough to show that no two of them are equal: supposing that $(f^i)^{j_1} = (f^i)^{j_2}$, we obtain $f^{i(j_1 - j_2)} = 1$, whence it follows that $n - 1$ divides $i(j_1 - j_2)$, since f is a primitive root.

(i) If i has no common factor with $n - 1$, it follows that $n - 1$ divides $j_1 - j_2$; given the range of values of j_1 and j_2, $0 \leq |j_1 - j_2| < n - 1$, so the only possibility is $j_1 = j_2$ and therefore all powers are indeed distinct, making f^i a primitive root.

(ii) If i has a common factor with $n - 1$, say s, then setting $j_1 - j_2 = (n - 1)/s$ we obtain that $i(j_1 - j_2) = i((n - 1)/s)$ is a multiple of $n - 1$; therefore, the powers

with, say, $j_1 = 0$, $j_2 = (n-1)/s < n-1$, are not distinct, hence f^i is not a primitive root.

The number of primitive roots of $\mathbb{F}$, then, is the number of i, $i = 1,\ldots,n-2$, without common factors with $n-1$; but this is precisely $\phi(n-1)$. This concludes the proof. □

In view of this theorem, it would be useful to have a tool to evaluate the Euler function. The following two theorems will provide exactly that.

Theorem 7.16. *Let $n = uv \in \mathbb{N}$, where u and v have no factors in common; then $\phi(n) = \phi(u)\phi(v)$.*

Proof. There are exactly $uv - \phi(uv)$, $u - \phi(u)$, $v - \phi(v)$, numbers having common factors with $uv = n$, u, and v, respectively, by the definition of ϕ. But a number can have a common factor with n if and only if it has a common factor with either u or v. Therefore, the numbers with common factors with n are exactly as many as those with a common factor with u plus those with a common factor with v minus those with a common factor with both, which we have counted twice. How many are in each category?

(i) A number from 1 up to and including n can have common factors with both u and v if and only if it can be written as ij, where i has common factors with u and j has common factors with v; this is because u and v have no factor in common. Hence, there are $(u - \phi(u))(v - \phi(v))$ such numbers.

(ii) A number can have common factors with u and be not greater than uv if it can be written as $ku + i$, where i has common factors with u and k takes the values from 0 to $v-1$ inclusive; there are $v(u - \phi(u))$ numbers.

(iii) Similarly, $u(v - \phi(v))$ numbers from 1 to n inclusive have common factors with v.

Therefore, $uv - \phi(uv) = v(u - \phi(u)) + u(v - \phi(v)) - (u - \phi(u))(v - \phi(v)) \Leftrightarrow \phi(uv) = \phi(u)\phi(v)$, and the proof is complete. □

Theorem 7.17. *Let p be a prime; then $\phi(p^m) = p^m(1 - 1/p)$, $m \in \mathbb{N}^*$, and $\phi(p) = p - 1$ as a special case.*

Proof. A number can have a common factor with p^m if and only if it is divisible by p, hence of the form ip, $i = 1,\ldots,p^{m-1}$; therefore, there are exactly p^{m-1} such numbers, which leaves $\phi(p^m) = p^m - p^{m-1} = p^m(1 - 1/p)$. Setting $m = 1$, $\phi(p) = p - 1$. □

Application 7.18. (i) $\phi(33) = \phi(3)\phi(11) = 2 \cdot 10 = 20$.

(ii) $\mathbb{F}_{17}$ has $\phi(16) = 2^3 = 8$ primitive roots.

(iii) $\mathbb{F}_{29}$ has $\phi(28) = \phi(4)\phi(7) = 6 \cdot 2 = 12$ primitive roots.

7.1.7. Logarithms on finite fields. The existence of primitive roots allows us to define *logarithms* on finite fields.

Definition 7.19. Let $\mathbb{F}$ be a finite field and x a primitive root. Then for all $y \in \mathbb{F} - \{0\}$, $u = \log_x(y) \in \{0,\ldots,|\mathbb{F}| - 2\} \Leftrightarrow x^u = y$.

This definition is sound: the set of powers $\{x^u \mid u = 0,\ldots,|\mathbb{F}|-2\}$ is equal to $\mathbb{F}-\{0\}$, as x is a primitive root of $\mathbb{F}$, which means that every element y can be written as a power x^u for exactly one u in the stated range of values.

7.1.8. Another family of finite fields. Are there more finite fields than $\mathbb{F}_p$ with p prime? We proved that there are not, as long as we insist on looking for them among the sets $\{1,\ldots,n\}$, $n \in \mathbb{N}^*$, with the usual definition of addition and multiplication. However, if the rules of the game change, we can find more indeed.

Definition 7.20. Let $\mathbb{F}_n^m = \{\sum_{i=0}^{m-1} a_i x^i \mid \text{for all } i \in \{0,\ldots,m-1\} a_i \in \mathbb{F}_n\}$, with $m,n \in \mathbb{N}^*$. This is the set of all polynomials of degree up to, but not including, m, with coefficients in $\mathbb{F}_n$. Define the sum of $a(x) = \sum_{i=0}^{m-1} a_i x^i, b(x) = \sum_{i=0}^{m-1} b_i x^i \in \mathbb{F}_n^m$ to be $(a+b)(x) = \sum_{i=0}^{m-1}((a_i+b_i) \bmod n)x^i$, and also define $ca(x) = \sum_{i=0}^{m-1}((ca_i) \bmod n)x^i$.

Apparently $\mathbb{F}_n^1 = \mathbb{F}_n$. Observe that $\mathbb{F}_n^{m_1} \subset \mathbb{F}_n^{m_2}$ if $m_2 > m_1$. The elements of these sets are polynomials, not numbers; this is the reason we avoided calling the elements of finite fields "numbers" whenever we discussed properties of finite fields in general: there exist, as we are about to see, finite fields whose elements are not numbers!

Definition 7.21. $\mathbb{F}_n^\infty = \bigcup_{m=0}^\infty \mathbb{F}_n^m$.

Theorem 7.22. *$\mathbb{F}_n^m$ is a vector space.*

Proof. If $f(x), g(x) \in \mathbb{F}_n^m$, then for all $a,b \in \mathbb{F}_n : af(x) + bg(x) \in \mathbb{F}_n^m$. □

This implies that it is a group under addition. The definition of the multiplication is a bit more involved, and it is based on the extension of the modulo function for polynomials.

Definition 7.23. Let $f(x) \in \mathbb{F}_n^m$, $g(x) \in \mathbb{F}_n^\infty$. Then, $f(x)$ modulo $g(x)$, $f(x) \bmod g(x)$, is defined to be the unique $r(x) \in \mathbb{F}_n^m$ that satisfies the following conditions:

(1) $\exists h(x) \in \mathbb{F}_n^\infty : f(x) = h(x)g(x) + r(x)$,

(2) $0 \le \text{degree}\,(r(x)) < \text{degree}\,(g(x))$.

Once more, we obtain that for all $h(x) \in \mathbb{F}_n^\infty, (f(x)+h(x)g(x)) \bmod g(x) = f(x) \bmod g(x)$ as an immediate consequence of the definition. Theorem 7.2 also has a counterpart.

Theorem 7.24. *For all $u(x), v(x) \in \mathbb{F}_n^m$, $g(x) \in \mathbb{F}_n^\infty$,*

(1) $(u(x)+v(x)) \bmod g(x) = (u(x) \bmod g(x) + u(x) \bmod g(x)) \bmod g(x)$,

(2) $(u(x)v(x)) \bmod g(x) = ((u(x) \bmod g(x))(v(x) \bmod g(x))) \bmod g(x)$.

Under what circumstances can $\mathbb{F}_n^m$ be a field? If n is not a prime, it certainly is not, for if $n = pq$, then $p,q \in \mathbb{F}_n^m$ and the modulo n multiplication implies that $(pq) \bmod n = n \bmod n = 0$, so that the product of two nonzero elements is 0, a contradiction. So n needs to be a prime.

If n is a prime, say $n = p$, we can prove that $\mathbb{F}_p^m$ can be turned into a field, by defining the multiplication modulo a suitable polynomial.

Definition 7.25. The product of $u(x), v(x) \in \mathbb{F}_p^m$ is defined to be

$$(uv)(x) = \big(u(x)v(x)\big) \bmod g(x), \tag{7.1}$$

where $g(x)$ is a polynomial in $\mathbb{F}_p^{m+1}$ of degree m, that is, with a nonzero highest power coefficient, which is taken to be 1.

If there exist two polynomials $g_1(x)$, $g_2(x)$ with coefficients in $\mathbb{F}_p$ and positive degrees so that $g_1(x)g_2(x) = g(x)$, then $g_1(x), g_2(x) \in \mathbb{F}_p^m$ and $(g_1 g_2)(x) = g(x) \bmod g(x) = 0$, so that the product of two nonzero elements is 0, a contradiction. Let us summarize.

Theorem 7.26. *If $\mathbb{F}_n^m$ is a field, then n is a prime and the polynomial $g(x)$ that defines the multiplication is irreducible, that is, it cannot be written as the product of polynomials of smaller positive degree with coefficients in $\mathbb{F}_n$.*

But if we do obey these restrictions, do we obtain a field? The answer is yes. First, we prove a preliminary result.

Theorem 7.27. *Let $f(x), g(x) \in \mathbb{F}_n^\infty$, for some $n \in \mathbb{N}^*$; consider the set $, S(f,g) = \{u(x)f(x) + v(x)g(x) | u(x), v(x) \in \mathbb{F}_p^\infty\}$, then, $S(f,g) = \{u(x)h(x) | u(x) \in \mathbb{F}_p^\infty\}$, where $h(x)$ is the greatest common divisor of $f(x)$, $g(x)$ with leading coefficient 1.*

Proof. If $s(x) \in S(f,g)$, then $h(x)$ divides $s(x)$. Consider the polynomial of least degree with leading coefficient 1 in $S(f,g)$, say $t(x)$ (it is unique); its degree is larger than or equal to the degree of $h(x)$, so we can divide them: $t(x) = h(x)d(x) + r(x)$ for some $d(x) \in \mathbb{F}_n^\infty$. But $h(x)$ divides $t(x)$, so it has to divide $r(x)$ as well, a contradiction since $r(x)$ has lower degree than $h(x)$. So, $r(x) = 0$ and $t(x) = d(x)h(x)$. But $f(x), g(x) \in S(f,g)$ themselves, so we can divide them by $t(x)$: $f(x) = d_f(x)t(x) + r_f(x)$ and $g(x) = d_g(x)t(x) + r_g(x)$; if r_f and r_g are not 0, we obtain members of $S(f,g)$ with degrees less than the degree of t, a contradiction. Hence, $t(x)$ divides $f(x)$ and $g(x)$, and therefore it is a common divisor of these two polynomials; so it divides the greatest common divisor $h(x)$. As these polynomials divide each other, they are equal $h(x) = t(x)$. So, every member of $S(f,g)$ is a multiple of $h(x)$ and the proof is complete. □

Theorem 7.28. *$\mathbb{F}_p^m$, with p prime, can be turned into a field by defining the multiplication of the polynomials that belongs in it modulo an irreducible polynomial $g(x)$.*

Proof. We have already proved all the defining properties of the field except the usual hard to get, the existence of multiplicative inverses. Let then $f(x) \in \mathbb{F}_p^m$, and consider the greatest common divisor of the two polynomials $f(x), g(x)$: as $g(x)$ has no divisors, being irreducible, the greatest common divisor in question is 1, and Theorem 7.27 guarantees the existence of two polynomials $u(x), v(x) \in \mathbb{F}_p^\infty$ so that $u(x)f(x) + v(x)g(x) = 1$, implying that $[u(x)f(x)] \bmod g(x) = 1$, that is, that $u(x) = (f(x))^{-1}$, and the proof is complete. □

$\mathbb{F}_p^m$ has exactly p^m elements: its polynomials have m coefficients, each of which can take p different values. It should be added that determining which ones among these elements are the primitive roots is a difficult problem (see an earlier note on that), as is the determination of an irreducible polynomial $g(x)$ to be used in the definition of the finite field (see [8] for a solution that was clearly associated with the ongoing at the time work on the algebraic construction of Costas arrays). Fortunately, for given p prime and m, both the irreducible polynomials of degree m over $\mathbb{F}_p$ and the primitive roots of $\mathbb{F}_p^m$

can be looked up in tables or in mathematical software, such as Matlab (we will see an example later).

7.2. Summary of results on finite fields.

(i) A field $\mathbb{F}$ is a set of elements along with two operations, addition and multiplication, defined on them, that obey the same familiar laws they obey on $\mathbb{R}$; in particular, it contains 0 and 1, and every element of the field other than 0 has a multiplicative inverse: for all $x \in \mathbb{F}, x \neq 0, \exists y \in \mathbb{F} : xy = 1$.

(ii) The set $\mathbb{F}_n = 0,1,\ldots,n-1$ with addition and multiplication defined as usual but modulo n is a field if and only if n is prime.

(iii) The set $\mathbb{F}_n^m = \{\sum_{i=0}^{m-1} a_i x^i \mid \text{for all } i \in \{0,\ldots,m-1\} a_i \in \mathbb{F}_n\}$, with $m,n \in \mathbb{N}^*$, that is, the set of all polynomials of degree up to m with coefficients in $\mathbb{F}_n$, is a field if and only if n is prime and the polynomial modulo which the multiplication is defined is irreducible.

(iv) In both cases the finite field $\mathbb{F}$ can be written as $\{0,1,x,\ldots,x^{|\mathbb{F}|-2}\}$, where x is an element of the field called a primitive root. All finite fields have primitive roots.

(v) For any field $\mathbb{F}$, any primitive root x, and any nonzero element y, there exists one number in $\{0,\ldots,|\mathbb{F}|-2\}$ called the logarithm of y with respect to x $\log_x(y)$, which is the power of x producing y: $x^{\log_x(y)} = y$.

7.3. The Welch construction. Welch found this algorithm of constructing Costas arrays heuristically; the correctness proof was published later by Golomb [9].

Theorem 7.29 (W_1). *Let $x \in \mathbb{F}_p - \{0,1\}$, p prime, be a primitive root; then, for any $s \in \{0,\ldots,p-2\}$, the permutation $f(s,1)\cdots f(s,p-1)$ with $f(s,i) = x^{i-1+s} \bmod p$, $i = 1,\ldots,p-1$, corresponds to a Costas array of order $p-1$.*

Proof. Let us take a look at two entries t_{ki} and t_{kj} on the same row of the difference triangle of the permutation: $t_{ki} = x^{i+s-1} \bmod p - x^{i+k+s-1} \bmod p$ and $t_{kj} = x^{j+s-1} \bmod p - x^{j+k+s-1} \bmod p$, with $1 \le i < i+k \le p-1$, $1 \le j < j+k \le p-1$, and $j \ge i$:

$$\begin{aligned} t_{ki} = t_{kj} &\iff x^{i-1+s} \bmod p - x^{i+k-1+s} \bmod p \\ &= x^{j-1+s} \bmod p - x^{j+k-1+s} \bmod p \Longrightarrow (x^{i-1+s} p - x^{i+k-1+s}) \bmod p \\ &= (x^{j-1+s} - x^{j+k-1+s}) \bmod p \iff (x^{i-1+s} - x^{i+k+s-1} - x^{j-1+s} + x^{j+k+s-1}) \bmod p \\ &= 0 \iff (x^{s-1}(x^i - x^j)(1-x^k)) \bmod p = 0 \Longrightarrow ((x^i - x^j)(1-x^k)) \bmod p = 0. \end{aligned} \tag{7.2}$$

It follows that p divides either $x^k - 1$ or $x^i - x^j$; but the former case leads to $x^k \bmod p = 1$ with $1 \le k < p-1$, which contradicts our assumption that x is a primitive root, and hence the second alternative must hold:

$$(x^i - x^j) \bmod p = 0 = [x^i(1-x^{j-i})] \bmod p \Longrightarrow (1-x^{j-i}) \bmod p = 0 \iff x^{j-i} \bmod p = 1. \tag{7.3}$$

If $j > i$, then $1 \leq j - i < p - 1$ and once more our assumption that x is a primitive root is contradicted; hence, $j = i$, and the proof is complete. □

Remark here that s is a rotation parameter: $f(s,1) \cdots f(s,p-1) = f(0,s) \cdots f(0,p-1) f(0,1) \cdots f(0,s-1)$. Based on this construction we obtain some more for free, by using Theorem 2.5.

Theorem 7.30 (W_2). *Let $x \in \mathbb{F}_p - \{0,1\}$ with p prime; then the permutation $f(2) - 1, \ldots, f(p-1) - 1$ with $f(i) = x^{i-1} \bmod p$, $i = 2, \ldots, p-1$, corresponds to a Costas array of order $p-2$.*

Proof. All constructions of W_1 with $s = 0$ start with 1; just remove it, and the remaining permutation is a Costas array, except that it contains the numbers 2 to $p-1$. As the Costas property does not depend on the numbers themselves but on their differences, we can redefine the permutation to contain the numbers 1 to $p-2$ by subtracting 1 from each of them. This completes the proof. □

Theorem 7.31 (W_3). *Consider $\mathbb{F}_p - \{0,1\}$ with p prime; if 2 is a primitive root of $\mathbb{F}_p$, then the permutation $f(3) - 2, \ldots, f(p-1) - 2$ with $f(i) = 2^{i-1} \bmod p$, $i = 3, \ldots, p-1$, corresponds to a Costas array of order $p-3$.*

Proof. Apply W_1 with $x = 2$ and $s = 0$; then $f(0,1) = 1$ and $f(0,2) = 2$. We just remove these two entries, and the remaining permutation is a Costas array, except that it contains the numbers 3 to $p-1$. As the Costas property does not depend on the numbers themselves but on their differences, we can redefine the permutation to contain the numbers 1 to $p-3$ by subtracting 2 from each of them. This completes the proof. □

There exists one last construction based on W_1, which works "sporadically" [12].

Theorem 7.32 (W_0). *Consider $\mathbb{F}_p - \{0,1\}$ with p prime; then, it is possible that there exists $s \in \{0, \ldots, p-2\}$ and a primitive root x so that the permutation $0 f(s,1) \cdots f(s,p-1)$ with $f(s,i) = x^{i-1+s} \bmod p$, $i = 1, \ldots, p-1$, corresponds to a Costas array of order p.*

Proof. By checking all possible cases we can prove that the method works for orders 19 and 31; in fact, the only Costas arrays produced by means of the construction algorithms in these orders are due to W_0. □

7.4. The Golomb construction. The Golomb construction works in the general finite fields $\mathbb{F}_p^m$, p prime, $m \in \mathbb{N}^*$.

7.4.1. Golomb methods

Theorem 7.33 (G_2). *Let a, b be two primitive roots, not necessarily distinct, of the field $\mathbb{F}_p^m$. Set $q = p^m$ and construct the permutation $f(1) \cdots f(q-2)$ by setting $f(i) = j$ if and only if $a^i + b^j = 1$, $i, j = 1, \ldots, q-2$; this permutation corresponds to a Costas array.*

Proof. Let us verify the result in steps. We will use the circled symbols for the field operations, to distinguish them from the usual real operations.

(i) For every $i \in \{1,\dots,q-2\}$ we can find a unique j satisfying the defining equality $a^i \oplus b^j = 1 \Rightarrow j = \log_b(1 \ominus a^i)$, and j cannot be 0 or else $1 \ominus a^i$ would be 1, and a^i would be 0, which is impossible; so $j \in \{1,\dots,q-2\}$ as well.

(ii) Let $j_1 = \log_b(1 \ominus a^{i_1})$, $j_2 = \log_b(1 \ominus a^{i_2})$, with $i_1 \geq i_2$. If $j_1 = j_2$, then $1 \ominus a^{i_1} = 1 \ominus a^{i_2} \Rightarrow a^{i_1 - i_2} = 1 \Rightarrow i_1 - i_2 = 0$, as $0 \leq i_1 - i_2 \leq q-2$. This proves that we cannot obtain the same j for two different i's.

(iii) Finally, we need to check the Costas property: consider the two entries t_{ki}, t_{kj}, which lie on the same row of the difference triangle of the permutation. More precisely, $t_{ki} = \log_b(1 \ominus a^i) - \log_b(1 \ominus a^{i+k})$ and $t_{kj} = \log_b(1 \ominus a^j) - \log_b(1 \ominus a^{j+k})$, $k = 1,\dots,q-3$, $1 \leq i \leq j \leq q-2$, $1 \leq i+k \leq j+k \leq q-2$. $t_{ki} = t_{kj}$ is equivalent to saying that

$$\begin{aligned}
&\log_b(1 \ominus a^i) - \log_b(1 \ominus a^{i+k}) \\
&\quad = \log_b(1 \ominus a^j) - \log_b(1 \ominus a^{j+k}) \Longleftrightarrow \log_b(1 \ominus a^i) + \log_b(1 \ominus a^{j+k}) \\
&\quad = \log_b(1 \ominus a^j) + \log_b(1 \ominus a^{i+k}) \Longleftrightarrow (1 \ominus a^i)(1 \ominus a^{j+k}) \\
&\quad = (1 \ominus a^j)(1 \ominus a^{i+k}) \Longrightarrow (1 \ominus a^i) \odot (1 \ominus a^{j+k}) \\
&\quad = (1 \ominus a^j) \odot (1 \ominus a^{i+k}) \Longleftrightarrow 1 \ominus a^i \ominus a^{j+k} \oplus a^{j+k+i} \\
&\quad = 1 \ominus a^j \ominus a^{i+k} \oplus a^{j+k+i} \Longleftrightarrow a^i \oplus a^{j+k} \\
&\quad = a^j \oplus a^{i+k} \Longleftrightarrow (1 \ominus a^k) \odot (a^i \ominus a^j) = 0.
\end{aligned} \tag{7.4}$$

This means that either $a^k = 1$ or $a^i = a^j \Leftrightarrow a^{j-i} = 1$; the former implies that $k = q-1$, which is impossible, whereas the latter means that $j - i = 0$, as $0 \leq j - i < q-2$.

This completes the proof. □

As in the Welch construction, we get some more constructions for free, using Theorem 2.5.

Theorem 7.34 (G_3). *Let a,b be two primitive roots, not necessarily distinct, of the field $\mathbb{F}_p^m$, with $a+b=1$. Set $q = p^m$, and construct the permutation $f(1)\cdots f(q-3)$ by setting $f(i) = j$ if and only if $a^{i+1} + b^{j+1} = 1$; this permutation corresponds to a Costas array.*

Proof. Applying G_2 with the two primitive roots $a,b : a+b=1$ means that $f(1) = 1$. Discard this entry, renumber $f(2)\cdots f(q-2)$ as $f(1)\cdots f(q-3)$, and subtract 1 from each remaining entry. The result is a Costas array of order $q-3$. □

Note that G_3 can always be applied if $q > 3$, for it can be shown that every such $\mathbb{F}_q$ contains primitive roots a and b such that $a+b=1$ [10].

Theorem 7.35 (G_4). *Let a,b be two primitive roots, not necessarily distinct, of the field $\mathbb{F}_2^m$, with $a+b=1$. Set $q = 2^m$, and construct the permutation $f(1)\cdots f(q-4)$ by setting $f(i) = j$ if and only if $a^{i+2} + b^{j+2} = 1$; this permutation corresponds to a Costas array.*

Proof. Applying G_2 with the two primitive roots $a,b : a+b=1$ means that $f(1) = 1$; moreover, as the arithmetic is modulo 2, $(a+b)^2 = 1^2 = 1 = a^2 + b^2 + ab + ab = a^2 + b^2$,

so $f(2) = 2$. Discard these entries, renumber $f(3)\cdots f(q-2)$ as $f(1)\cdots f(q-4)$, and subtract 2 from each remaining entry. The result is a Costas array of order $q-4$. □

Theorem 7.36 (G_4^*). *Let a, b be two primitive roots, not necessarily distinct, of the field $\mathbb{F}_p^m$, with $a+b=1$, $a^2+b^{-1}=1$. Set $q=p^m$, and construct the permutation $f(1)\cdots f(q-4)$ by setting $f(i)=j$ if and only if $a^{i+2}+b^{j+1}=1$; this permutation corresponds to a Costas array.*

Proof. Applying G_2 with the two primitive roots $a,b : a+b=1$ means that $f(1)=1$; moreover, $b^{-1}=b^{q-2}$ since $b^{q-1}=1$, which implies that $f(2)=q-2$. Discard these entries, renumber $f(3)\cdots f(q-2)$ as $f(1)\cdots f(q-4)$, and subtract 1 from each remaining entry. The result is a Costas array of order $q-4$. □

Note that the values of q for which G_4^* occurs are either 4, 5, and 9, or those primes p for which T_4 occurs (see below) and which satisfy $p \bmod 20 = 1$ or 9 [10].

Theorem 7.37 (G_5^*). *Let a, b be two primitive roots, not necessarily distinct, of the field $\mathbb{F}_p^m$, with $a+b=1$, $a^2+b^{-1}=1$. Set $q=p^m$, and construct the permutation $f(1)\cdots f(q-5)$ by setting $f(i)=j$ if and only if $a^{i+2}+b^{j+2}=1$; this permutation corresponds to a Costas array.*

Proof. Applying G_2 with the two primitive roots $a,b : a+b=1$ means that $f(1)=1$; moreover, $b^{-1}=b^{q-2}$ since $b^{q-1}=1$, which implies that $f(2)=q-2$.

What is more, $b^2+a^{-1}=1$. In order to see this, multiply the two relations on a, b to get $(a+b)(a^2+b^{-1})=1\cdot 1=1=a^3+ba^2+ab^{-1}+1 \Rightarrow a^2+b^{-1}=-ab$, whence it follows that $ab=-1$. Then, $a+b=1 \Rightarrow 1+ba^{-1}=a^{-1}=1+b^2(ab)^{-1}=1-b^2 \Rightarrow a^{-1}+b^2=1$. This proves that $f(q-2)=2$.

Discard these three entries in the order listed, renumber $f(3)\cdots f(q-3)$ as $f(1)\cdots f(q-5)$, and subtract 2 from each remaining entry. The result is a Costas array of order $q-5$. □

7.4.2. Lempel methods. Historically, the special case of G_2 with $a=b$ was first discovered heuristically by A. Lempel, and therefore it bears the name of *the Lempel construction*. Lempel constructions have the property that they lead to symmetric Costas arrays.

Theorem 7.38 (L_2). *Let a be a primitive root of the field $\mathbb{F}_p^m$. Set $q=p^m$, and construct the permutation $f(1)\cdots f(q-2)$ by setting $f(i)=j$ if and only if $a^i+a^j=1$; this permutation corresponds to a Costas array.*

Theorem 7.39 (L_3). *Suppose 2^{-1} is a primitive root of the field $\mathbb{F}_p^m$. Set $q=p^m$, and construct the permutation $f(1)\cdots f(q-3)$ by setting $f(i)=j$ if and only if $2^{-(i+1)}+2^{-(j+1)}=1$; this permutation corresponds to a Costas array.*

Proof. Apply L_2 with $a=2^{-1}$. Observe that $2^{-1}+2^{-1}=1$, hence $f(1)=1$. Discard this entry, renumber $f(2)\cdots f(q-2)$ as $f(1)\cdots f(q-3)$, and subtract 1 from each remaining entry. The result is a Costas array of order $q-3$. □

7.4.3. Taylor methods. The *Taylor constructions* are based on the Welch and Lempel constructions, and are due to Taylor [10, 12].

THEOREM 7.40 (T_4). *Let a be a primitive root of the field $\mathbb{F}_p^m$, with the property that $a^2 + a = 1$. Set $q = p^m$, and construct the permutation $f(1)\cdots f(q-4)$ by setting $f(i) = j$ if and only if $a^{i+2} + a^{j+2} = 1$; this permutation corresponds to a Costas array.*

Proof. Apply L_2 with a; the property of a implies that $f(1) = 2$ and $f(2) = 1$. Discard these entries, renumber $f(3)\cdots f(q-2)$ as $f(1)\cdots f(q-4)$, and subtract 2 from each remaining entry. The result is a Costas array of order $q-4$. □

Note that it is shown in [10] that a necessary condition for T_4 to work is that q be either 4, 5, or 9, or a prime p so that $p \bmod 10 = \pm 1$.

Let $P = f(1)\cdots f(q-2)$, $q = p^m$, p prime, be constructed according to G_2 with primitive roots a and b. We would like to investigate under which circumstances it is possible to add an $f(0)$ or an $f(q-1)$. Our first observation already is that the value of this addition will need to be either 0 or $q-1$, hence we end up with 4 possible different cases.

(1) The addition of $f(0) = 0$ will fail if and only if $\exists x_1, x_2, y_1, y_2 \in \{1,\ldots,p-2\}$ so that $f(x_1) = y_1$, $f(x_2) = y_2$, $x_1 + x_2 < q-1$, and $f(0) - f(x_1) = f(x_2) - f(x_1 + x_2) \Leftrightarrow 0 - y_1 = y_2 - f(x_1 + x_2) \Leftrightarrow f(x_1 + x_2) = y_1 + y_2 < q-1$. The relations defining the construction of G_2 give $a^{x_1} + b^{y_1} = 1$, $a^{x_2} + b^{y_2} = 1$, and $a^{x_1+x_2} + b^{y_1+y_2} = 1$. By multiplying the first two and subtracting the third, we get $a^{x_1} b^{y_2} + a^{x_2} b^{y_1} = 0 \Leftrightarrow a^{x_1-x_2} + b^{y_1-y_2} = 0$.

(2) The addition of $f(0) = q-1$ will fail if and only if $\exists x_1, x_2, y_1, y_2 \in \{1,\ldots,p-2\}$ so that $f(x_1) = y_1$, $f(x_2) = y_2$, $x_1 + x_2 < q-1$, and $f(0) - f(x_1) = f(x_2) - f(x_1 + x_2) \Leftrightarrow q - 1 - y_1 = y_2 - f(x_1 + x_2) \Leftrightarrow f(x_1 + x_2) = y_1 + y_2 + 1 - q$. The relations defining the construction of G_2 give $a^{x_1} + b^{y_1} = 1$, $a^{x_2} + b^{y_2} = 1$, and $a^{x_1+x_2} + b^{y_1+y_2+1-q} = 1 = a^{x_1+x_2} + b^{y_1+y_2}$, because $b^{q-1} = 1$. By multiplying the first two and subtracting the third, we get $a^{x_1} b^{y_2} + a^{x_2} b^{y_1} = 0 \Leftrightarrow a^{x_1-x_2} + b^{y_1-y_2} = 0$. Finally, $0 < y_1 + y_2 + 1 - q < q-1 \Leftrightarrow q \le y_1 + y_2 < 2(q-1)$.

(3) The addition of $f(q-1) = 0$ will fail if and only if $\exists x_1, x_2, y_1, y_2 \in \{1,\ldots,p-2\}$ so that $f(q-1-x_1) = q-1-y_1$, $f(q-1-x_2) = q-1-y_2$, $x_1 + x_2 < q-1$, and $f(q-1-x_1-x_2) - f(q-1-x_2) = f(q-1-x_1) - f(q-1) \Leftrightarrow f(q-1-x_1-x_2) = 2(q-1) - y_1 - y_2$. The relations defining the construction of G_2 give $a^{q-1-x_1} + b^{q-1-y_1} = 1 = a^{-x_1} + b^{-y_1}$, $a^{q-1-x_2} + b^{q-1-y_2} = 1 = a^{-x_2} + b^{-y_2}$, and $a^{q-1-x_1-x_2} + b^{2(q-1)-y_1-y_2} = 1 = a^{-(x_1+x_2)} + b^{-(y_1+y_2)}$, because $b^{q-1} = 1$. By multiplying the first two and subtracting the third, we get $a^{-x_1} b^{-y_2} + a^{-x_2} b^{-y_1} = 0 \Leftrightarrow a^{x_2-x_1} + b^{y_2-y_1} = 0$. Finally, $0 < 2(q-1) - y_1 - y_2 < q-1 \Leftrightarrow q \le y_1 + y_2 < 2(q-1)$.

(4) The addition of $f(q-1) = q-1$ will fail if and only if $\exists x_1, x_2, y_1, y_2 \in \{1,\ldots,p-2\}$ so that $f(q-1-x_1) = q-1-y_1$, $f(q-1-x_2) = q-1-y_2$, $x_1 + x_2 < q-1$, and $f(q-1-x_1-x_2) - f(q-1-x_2) = f(q-1-x_1) - f(q-1) \Leftrightarrow f(q-1-x_1-x_2) = q-1-y_1-y_2$. The relations defining the construction of G_2 give $a^{q-1-x_1} + b^{q-1-y_1} = 1 = a^{-x_1} + b^{-y_1}$, $a^{q-1-x_2} + b^{q-1-y_2} = 1 = a^{-x_2} + b^{-y_2}$, and $a^{q-1-x_1-x_2} + b^{q-1-y_1-y_2} = 1 = a^{-(x_1+x_2)} + b^{-(y_1+y_2)}$, because $b^{q-1} = 1$. By multiplying the first two and subtracting the third, we get $a^{-x_1} b^{-y_2} + a^{-x_2} b^{-y_1} = 0 \Leftrightarrow a^{x_2-x_1} + b^{y_2-y_1} = 0$. Finally, $0 < (q-1) - y_1 - y_2 < q-1 \Leftrightarrow 1 \le y_1 + y_2 < q-1$.

Since a is a primitive root of $\mathbb{F}_p^m$, there exists a $k<p-1$ so that $b=a^k$. The final equations of the 4 steps above can be written in the form $a^{\Delta x} + b^{\Delta y} = 0 \Leftrightarrow a^{\Delta x} = -a^{k\Delta y} = a^{k\Delta y \pm (q-1)/2}$,

because 2 divides $q-1$, $(a^{(q-1)/2})^2 = a^{q-1} = 1$, and $(q-1)/2 \neq 0$, so necessarily $a^{(q-1)/2} = -1$. Therefore,

$$(x_1 - x_2) \bmod (q-1) = \left\lfloor k(y_1 - y_2) + \frac{q-1}{2} \right\rfloor \bmod (q-1). \tag{7.5}$$

Moreover, because b is a primitive root too and $b = a^k$, k cannot have common factors with $q-1$ (they need to be *coprime*); otherwise, if the greatest common divisors of b and $q-1$ were $d > 1$, then $b^{(q-1)/d} = a^{k(q-1)/d} = (a^{q-1})^{k/d} = 1$ and $(q-1)/d < q-1$, a contradiction.

We have proved the following theorem.

Theorem 7.41 (Corner conditions). *Let $P = f(1)\cdots f(q-2)$, $q = p^m$, p prime, be constructed according to G_2 with primitive roots a and b. Then*

(1) *the permutation $f(0)f(1)\cdots f(q-2)$ with $f(0) = 0$ will not be a Costas array if and only if $\exists x_1, x_2, y_1, y_2 \in \{1,\ldots,p-2\}$ so that $f(x_1) = y_1$, $f(x_2) = y_2$, $x_1 + x_2 < q-1$, $f(x_1 + x_2) = y_1 + y_2$, $y_1 + y_2 < q-1$, and (7.5) holds;*

(2) *the permutation $f(0)f(1)\cdots f(q-2)$ with $f(0) = q-1$ will not be a Costas array if and only if $\exists x_1, x_2, y_1, y_2 \in \{1,\ldots,p-2\}$ so that $f(x_1) = y_1$, $f(x_2) = y_2$, $x_1 + x_2 < q-1$, $f(x_1 + x_2) = y_1 + y_2 - q + 1$, $q \leq y_1 + y_2 < 2(q-1)$, and (7.5) holds;*

(3) *the permutation $f(1)\cdots f(q-2)f(q-1)$ with $f(q-1) = 0$ will not be a Costas array if and only if $\exists x_1, x_2, y_1, y_2 \in \{1,\ldots,p-2\}$ so that $f(q-1-x_1) = q-1-y_1$, $f(q-1-x_2) = q-1-y_2$, $x_1 + x_2 < q-1$, $f(q-1-x_1-x_2) = 2(q-1) - y_1 - y_2$, $q \leq y_1 + y_2 < 2(q-1)$, and (7.5) holds;*

(4) *the permutation $f(1)\cdots f(q-2)f(q-1)$ with $f(q-1) = q-1$ will not be a Costas array if and only if $\exists x_1, x_2, y_1, y_2 \in \{1,\ldots,p-2\}$ so that $f(q-1-x_1) = q-1-y_1$, $f(q-1-x_2) = q-1-y_2$, $x_1 + x_2 < q-1$, $f(q-1-x_1-x_2) = q-1-y_1-y_2$, $1 \leq y_1 + y_2 < q-1$, and (7.5) holds.*

The name of the theorem derives from the dot representation of a permutation: a dot exists at (j,i) if and only if $f(i) = j$, and therefore the extensions mentioned in the theorem correspond to adding a dot at one of the four corners of the array.

We have now proved T_1.

Theorem 7.42 (T_1). *If $f(1)\cdots f(q-2)$ is generated by the application of G_2, then it is possible to obtain a Costas array of order $q-1$ by setting one of the following: $f(0) = 0$ or $f(0) = q-1$ or $f(q-1) = 0$ or $f(q-1) = q-1$, unless the corner conditions prevent it.*

Two dots may also be added occasionally.

Theorem 7.43 (T_0). *If $f(1)\cdots f(q-2)$ is generated by the application of G_2, then it is possible to obtain a Costas array of order q by setting one of the following pairs: $f(0) = 0$ and $f(q-1) = q-1$, or $f(q-1) = 0$ and $f(0) = q-1$, as long as the corner conditions do not prevent it.*

Proof. The possibility is proved by the fact that it works for $q = 47$ [12]. □

Table 7.1

i	x^i	i	x^i	i	x^i
0	1	5	x^2+x	10	x^2+x+1
1	x	6	x^3+x^2	11	x^3+x^2+x
2	x^2	7	x^3+x+1	12	x^3+x^2+x+1
3	x^3	8	x^2+1	13	x^3+x^2+1
4	$x+1$	9	x^3+x	14	x^3+1

Numerous other results are offered in [12, 23], which investigate the applicability of the various constructions that are not unconditionally applicable, such as T_0 and T_1 above, for specific families of numbers. As the proofs are quite technical and the results are of limited practical value they will not be reproduced here.

7.5. Construction examples. Let us apply here the basic methods W_1 and L_2 to construct two Costas arrays. We will use $p = 17$ and $q = 2^4 = 16$, respectively, so that W_1 will yield a Costas array of order 16, and L_2 one of order 14.

In order to apply W_1 we need to find a primitive root of $\mathbb{F}_{17}$; we test 2 and it fails, as the order of the cyclic group generated by 2 turns out to be 8; then we test 3 and it succeeds, because the powers $f(i) = 3^{i-1} \bmod 17$, $i = 1,\ldots,16$, are all different. The Costas array generated by W_1 is $\boxed{1\,3\,9\,10\,13\,5\,15\,11\,16\,14\,8\,7\,4\,12\,2\,6}$.

The application of L_2 is a bit more involved.

(i) First of all, we need to find an irreducible polynomial of $\mathbb{F}_2^4$: such polynomials are well tabulated in books and software; for example, Matlab has the command "gfprimfd" for this purpose, which yields all irreducible polynomials over a finite field. If we run it, we find that $P(x) = x^4 + x + 1$ is such a polynomial.

(ii) Now we need a primitive root of the field: a good idea is to test x as a start, as it is the simplest possible polynomial. It turns out to be a primitive root. The computation of the powers follows the recursion $x^0 = 1$, and $x^i = (xx^{i-1} \bmod(x^4 + x + 1))$, $i = 1,\ldots,14$; in practice this means that we find x^i as the product xx^{-1}, and then we substitute x^4, if it appears, by $x + 1$. Table 7.1 is the full table, which can equally well be used as the logarithm table.

We need to solve the equation $x^i + x^j = 1$, $j = f(i)$ for $i = 1,\ldots,14$, to find the L_2 construction of a Costas array of order 14; fortunately, we need only 7 calculations, as L_2 generates symmetric Costas arrays:

(1) $x + x^j = 1 \Leftrightarrow x^j = 1 + x \Leftrightarrow j = 4$,
(2) $x^2 + x^j = 1 \Leftrightarrow x^j = 1 + x^2 \Leftrightarrow j = 8$,
(3) $x^3 + x^j = 1 \Leftrightarrow x^j = 1 + x^3 \Leftrightarrow j = 14$,
(4) $x^5 + x^j = 1 = x^2 + x + x^j \Leftrightarrow x^j = 1 + x + x^2 \Leftrightarrow j = 10$,
(5) $x^6 + x^j = 1 = x^3 + x^2 + x^j \Leftrightarrow x^j = 1 + x^2 + x^3 \Leftrightarrow j = 13$,
(6) $x^7 + x^j = 1 = x^3 + x + 1 + x^j \Leftrightarrow x^j = x^3 + x \Leftrightarrow j = 9$,
(7) $x^{11} + x^j = 1 = x^3 + x^2 + x + x^j \Leftrightarrow, x^j = x^3 + x^2 + x + 1 \Leftrightarrow j = 12$.

The Costas array generated is then $\boxed{4\,8\,14\,1\,10\,13\,9\,2\,7\,5\,12\,11\,6\,3}$.

8. Trial and error: 1-Gap augmentation [18]

Assume that $P = f(1)\cdots f(n)$, $f : \{1,\ldots,n\} \to \{1,\ldots,n\}$, f a bijection, corresponds to a Costas array; we can attempt to create a $P' = g(1)\cdots g(n+1)$, g a bijection, that corresponds to a Costas array of one order higher by the following process.

(1) Apply the following steps to all $P_i = f_i(1)\cdots f_i(n)$, $i = 0,1,\ldots,n-1$, where $f_i(k) = (k+i-1) \bmod n + 1$.
(2) Apply the following step for all $j = 1,\ldots,n+1$.
(3) (a) For every k, if $f_i(k) \geq j$ set $g(k) = f_i(k) + 1$, otherwise set $g(k) = f_i(k)$.
    (b) Set $g(n+1) = j$, and test whether the $P' = g(1)\cdots g(n+1)$ so defined is Costas; then test whether $P'' = g(n+1)g(1)\cdots g(n)$ is Costas.

In terms of the dot representation of the permutation, these operations amount to "rolling" or shifting the array dots in the vertical direction, then "cutting" the matrix horizontally to introduce one more row, and finally appending one more column to the left or to the right, with its dot lying on the new row.

Let us demonstrate the process with an example: the permutation $P = 4213$ is Costas, as one can easily check. Consider $P_1 = 1324$, which results from P by rolling its dots one position upwards; it is not Costas, but it does not matter. Create a new permutation by increasing all entries larger than or equal to 2 by 1: 1435, that is, by choosing $j = 2$ in step 3 of the algorithm above. Finally, append 2 once on the left and once on the right to obtain $P' = 21435$ and $P'' = 14352$. After testing, we discover that the former is not Costas, while the latter is.

This method has yielded 4 new Costas arrays of order up to and including 100, the definition of new being that they had not been obtained before through exhaustive search or the construction algorithms: 2 of order 29, 1 of 36, and 1 of 42. These constructions are shown below.

3 21 23 22 8 15 26 6 16 11 28 5 2 18 10 14 12 13 27 20 9 29 19 24 7 1 4 17 25

4 12 25 28 22 5 10 29 20 9 2 16 17 15 19 11 27 24 1 18 13 23 3 14 21 7 6 8 26

2 29 33 19 21 27 32 9 1 30 17 36 16 23 14 12 24 5 31 6 26 15 18 28 22 7 25 3 11 20 8 4 35 34 13 10

3 6 29 34 36 27 13 30 2 40 14 41 39 22 19 31 4 28 18 7 8 1 12 21 20 26 42 24 37 15 25 33 17 35 23 10 5 9 16 38 32 11

The theoretical justification of these manipulations is the following theorem, for which more details can be found in [18].

THEOREM 8.1. *Let P be a Costas array generated according to W_1 or G_2; then the sequence of numbers produced at the end of Step (3)(a) above satisfies the Costas property.*

Even without this theorem, though, one would be totally justified to use the algorithm above as a "clever brute force" method to search for Costas arrays: it is clear that all the operations involved in the algorithm preserve more or less the Costas structure, namely a low number of repetitions of entries in the rows of the difference triangle, which occasionally may be 0 so that a Costas array is produced. In other words, instead of searching

"blindly" for Costas arrays, as in the exhaustive search, it may be more efficient to start with constructions that are "almost" Costas, such as the ones produced by the algorithm above, and test only them.

9. Open questions

During the past decades many conjectures were formulated on Costas arrays. Some of them were subsequently proved or disproved, but it would be no exaggeration to say that most of them, and, among them, the most important ones, remain still open.

(1) For all $n \in \mathbb{N}^*$, $n \geq 2$, $\mathcal{C}_n \neq \emptyset$; or in the form of a question: *are there Costs arrays for all orders?*

The issue arises because the orders for which, according to the construction algorithms, Costas arrays can be constructed contain some "gaps". Actually, this is rather the picture for "small" orders, say less than 100; because for large orders, as primes and powers of primes are sparse within the integers, it would probably be more accurate to say that in general the algorithms do not work, but that occasionally there are small "islands" of consecutive integers for which they do. An invaluable table of which constructions work at which orders, for orders up to 360, is given in [12]: we promptly learn that for orders $n \leq 100$, the algorithms yield nothing at $n = 32, 33, 43, 48, 49, 54, 63, 73, 74, 83$–$85, 89$–$93, 97$. We reproduce this table up to order 50 here, as Table 9.1.

The case of $n = 53$ deserves a special mention, due to its peculiar history. Originally [12] included it in the list above, although this is clearly a mistake: W_0 does yield a Costas array for $n = 53$; this fact was discovered by Carbonera, a student of Moreno's, before 1986 [3, 17], but apparently it was not immediately published, as the the first mention of this construction in the literature that we can trace of appears in [25], dating 1995 and written in Chinese; it is only in 2003 that it appears again in [16], in the western literature this time, but Carbonera's name is not explicitly mentioned.

32 is tantalizingly close to 25, today's bound of successful exhaustive search, so one might be tempted to think that by pushing exhaustive search a bit, the answer to the great mystery of whether Costas arrays exist for all orders could be revealed. Unfortunately, the factorial increase in complexity of exhaustive search, much faster than the exponential increase of Moore's Law for the increase of speed of our computer resources [1], does not allow us to be very optimistic that order 32 will be tackled soon (although members of Beard's group do have expressed some optimism on this point).

In the meantime, both sides seem to keep their hopes up: the author of [13], after listing the orders below 100 for which constructions do not work, proceeds to state that "[o]ur goal is to fill these gaps", which can be construed to presuppose the optimistic view that this is indeed possible; at the same time period, the author of [1] conjectures that there are infinitely many orders for which Costas arrays fail to exist, which is clearly pessimistic.

(2) *Are there other construction algorithms, perhaps not based on finite field techniques?*

Some incidents seem to suggest that very often the construction algorithms seem to capture a very small fraction of the total number of Costas arrays for a given order. For example, the construction table in [12] shows that for orders 19 and 31 the only known examples of Costas arrays originating from the algorithms result from the "sporadic" W_0.

Table 9.1. Constructions that successfully produce Costas arrays for order ≤ 50 (copied from [12]).

Order	Working constructions	Order	Working constructions
—	—	26	W_3, L_3, G_3
—	—	27	W_2, L_2, T_4, G_2
3	T_1, W_2, L_2, G_2	28	T_1, W_1, G_3, G_4
4	$T_1, W_1, G_3, G_4, G_5^*$	29	T_0, W_2, L_2, G_2, G_3
5	$T_0, W_2, L_2, T_4, G_2, G_3, G_4^*$	30	W_1, L_2, G_2
6	T_1, W_1, L_2, G_2, G_3	31	W_0
7	W_0, L_2, T_4, G_2	32	—
8	T_1, W_3, L_3, G_3	33	—
9	W_2, L_2, G_2	34	W_3, L_3, G_3
10	T_2, W_1, W_3, L_3, G_3	35	W_2, L_2, G_2
11	T_0, W_2, L_2, G_2	36	W_1, G_5^*
12	W_1, G_4	37	T_4, G_4^*
13	W_0, G_3	38	G_3
14	L_2, G_2, G_3	39	W_2, L_2, G_2
15	W_2, L_2, T_4, G_2	40	W_1, G_3
16	T_1, W_1, W_3, L_3, G_3	41	W_2, L_2, G_2
17	T_0, W_2, L_2, G_2	42	W_1
18	W_1	43	—
19	W_0	44	G_3
20	G_3	45	W_2, L_2, G_2
21	W_2, L_2, G_2	46	T_1, W_1, G_3
22	T_1, W_1, G_3	47	T_0, L_2, G_2
23	T_0, L_2, G_2	48	—
24	G_3	49	—
25	L_2, G_2	50	W_3, L_3, G_3

Today, the example for 31 is still the only known Costas array for that order, modulo the symmetry; but 19 has been covered by the exhaustive search, which yielded 10240 Costas arrays at that order! Where did all the others come from?

In particular, all algorithms for Costas arrays published today, with the exception of the 1-Gap augmentation, seem to be polarized at the two extremes: on the brute force side lies the exhaustive search, while on the purely mathematical side lie the construction algorithms. No attempt of a "clever" search has been published, for example.

(3) *Is it the case that for sufficiently large orders the only existing Costas arrays are the ones produced by the construction algorithms?*

A simple counting argument reveals the reason for this question: a Costas array of order n is defined by the n numbers $1,\ldots,n$, the order of which needs to obey $O(n^3)$ restrictions, according to Theorem 4.3. As the number of restrictions rises much faster than the number of available integers, higher-order Costas arrays are much more constrained than lower-order ones. Therefore, all lower-order Costas arrays not produced by the algorithms can be treated as "accidentals," for which there is no room in higher orders.

1-Gap augmentation proves that, if this conjecture is true, then the sufficiently large orders start above order 42.

(4) *Is there a closed formula for* $|\mathcal{C}_n|$*?*

(5) *Is there a simple way to determine whether there exist Costas arrays for a particular order?*

10. Conclusion

Costas arrays can be truly fascinating objects for a mathematician interested in discrete mathematics, as, on the one hand, their theory involves interesting mathematics, and, on the other, the fundamental problems of existence and construction are still not fully solved. Moreover, they are also appealing to engineers, because of their applications in radar and sonar engineering, which actually where they originated from. As no new method of construction has emerged in the last 20 years, except 1-Gap augmentation with its limited success in low orders, and as our capability for exhaustive search seems to have saturated, it seems now reasonable to try to adopt alternative approaches, such as "clever brute force" methods or randomized methods.

It should be noted that Costas arrays have not been studied out of the wider context of positioning problems in discrete mathematics: connections have been found with non-attacking Kings, Queens [12], and Rooks [23] in chess, Vatican and Florentine arrays [21], Tuscan arrays [7, 11], and so forth, through which important contributions have been made to Costas arrays themselves. We can expect that such connections will contribute to answering the still unanswered questions on them.

In the meantime, we can only hope that this article has successfully achieved its goal, which was the presentation of (almost) everything basic we know today on Costas arrays, these elusive beasts of the mathematical kingdom.

Acknowledgments

The author would like to thank Dr. Scott Rickard of the Department of Electrical Engineering of University College of Dublin for introducing him to the problem, and providing him with data and papers [1, 18]; he would also like to thank Dr. Liam O'Caroll of the School of Mathematics of the University of Edinburgh for providing him with a paper on the subject [13]; finally, he would like to thank the anonymous reviewers, who suggested some further references and some interesting details on the history of Costas arrays, and Professor Oscar Moreno of the University of Puerto Rico for confirming some of these details.

References

[1] J. K. Beard, *Combinatoric collaboration on Costas arrays and radar applications*, Slide presentation in RADARCON, 2004.

[2] J. K. Beard, J. C. Russo, K. Erickson, M. Monteleone, and M. Wright, *Combinatoric collaboration on Costas arrays and radar applications*, IEEE National Radar Conference, Pennsylvania, 2004, pp. 260–265.

[3] P. Carbonera Pardo, *Arreglos de Costa Tamaño P*, Presentation in the 21st ACS Junior Technical Meeting—6th Interdisciplinary Scientific Meeting of Puerto Rico, April 1986.

[4] W. Chang, *A remark on the definition of Costas arrays*, Proceedings of the IEEE **75** (1987), no. 4, 522–523.

[5] J. P. Costas, *A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties*, Proceedings of the IEEE **72** (1984), no. 8, 996–1009.

[6] ———, *Medium constrains on sonar design and performance*, Technical Report Class 1 Rep. R65EMH33, GE Company.

[7] T. Etzion, S. W. Golomb, and H. Taylor, *Tuscan-K squares*, Advances in Applied Mathematics **10** (1989), no. 2, 164–174.

[8] S. W. Golomb, *Obtaining specified irreducible polynomials over finite fields*, SIAM Journal on Algebraic and Discrete Methods **1** (1980), no. 4, 411–418.

[9] ———, *Algebraic constructions for Costas arrays*, Journal of Combinatorial Theory. Series A **37** (1984), no. 1, 13–21.

[10] ———, *The T_4 and G_4 constructions for Costas arrays*, IEEE Transactions on Information Theory **38** (1992), no. 4, 1404–1406.

[11] S. W. Golomb, T. Etzion, and H. Taylor, *Polygonal path constructions for Tuscan-k squares*, Ars Combinatoria **30** (1990), 97–140.

[12] S. W. Golomb and H. Taylor, *Constructions and properties of Costas arrays*, Proceedings of the IEEE **72** (1984), no. 9.

[13] D. Huw Davies, *On the density of Costas arrays*, IEEE Transactions on Information Theory (1989).

[14] J. Johnsen, *On the distribution of powers in finite fields*, Journal für die reine und angewandte Mathematik **251** (1971), 10–19.

[15] O. Moreno, *On primitive elements of trace equal to* 1 *in* GF(2^m), Discrete Mathematics **41** (1982), no. 1, 53–56.

[16] ———, *Survey on Costas arrays and their generalizations*, Mathematical Properties of Sequences and Other Combinatorial Structures (Los Angeles, Calif, 2002), Kluwer Academic, Massachusetts, 2003, pp. 55–64.

[17] ———, personal communication, 2006.

[18] S. Rickard, *Searching for Costas arrays using periodicity properties*, IMA International Conference on Mathematics in Signal Processing, The Royal Agricultural College, Cirencester, December 2004.

[19] ———, personal communication, 2005.

[20] J. Silverman, V. E. Vickers, and J. M. Mooney, *On the number of Costas arrays as a number of array size*, Proceedings of the IEEE **76** (1988), no. 7, 851–853.

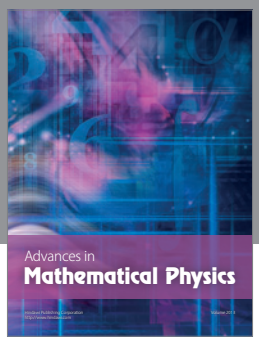
[21] H. Y. Song and S. W. Golomb, *Generalized Welch-Costas sequences and their application to Vatican arrays*, Finite Fields: Theory, Applications, and Algorithms (Las Vegas, Nevada, 1993), Contemporary Mathematics, vol. 168, American Mathematical Society, Rhode Island, 1994, pp. 341–351.

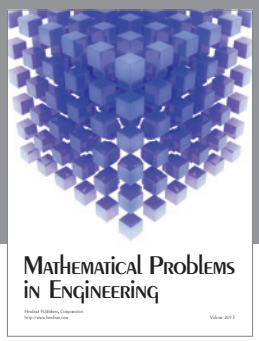
[22] M. Szalay, *On the distribution of the primitive roots of a prime*, Journal of Number Theory **7** (1975), no. 2, 184–188.

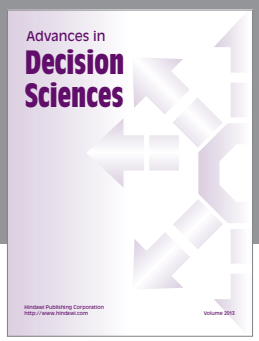
[23] H. Taylor, *Non-attacking Rooks with distinct differences*, Tech. Rep. CSI-84-03-2, EE Systems, University of Southern California, California.

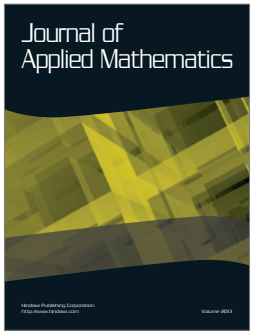
[24] E. Vegh, *A note on the distribution of the primitive roots of a prime*, Journal of Number Theory **3** (1971), no. 1, 13–18.
[25] Y. Zhenghua, O. Jianquan, and H. Rongjun, *The discovery of* 53×53 *Costas arrays*, Natural Science Journal of Xiangtan University **17** (1995), no. 4, 120–122 (Chinese).

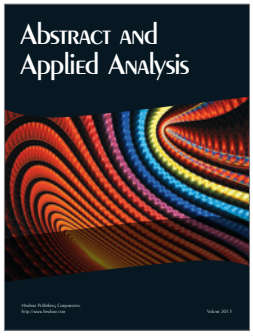
Konstantinos Drakakis: School of Mathematics, University of Edinburgh, James Clerk Maxwell Building, The King's Buildings, Mayfield Road, Edinburgh EH9 3JZ, Scotland, UK
E-mail address: k.drakakis@ed.ac.uk

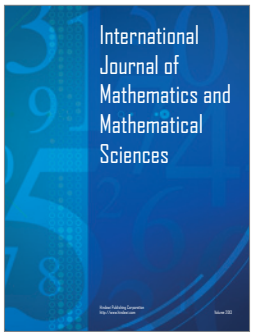


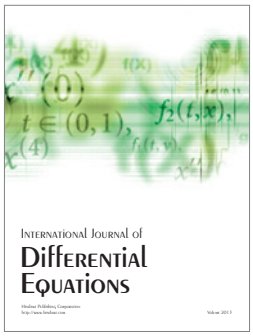


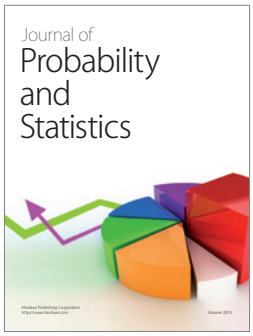


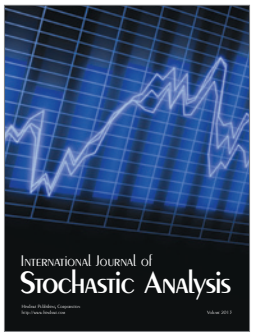


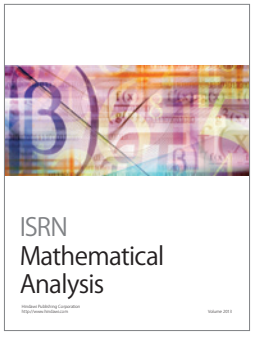


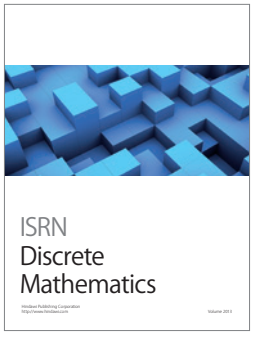


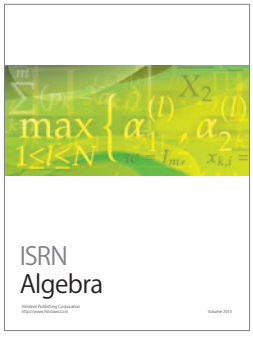


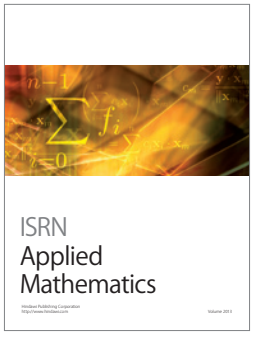


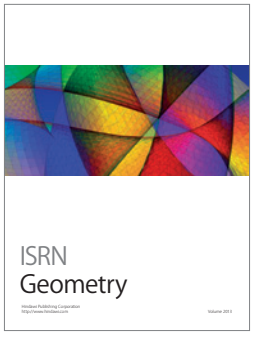












Hindawi
Submit your manuscripts at
http://www.hindawi.com